EMG5324-D10A

Wireless N GbE VoIP IAD with USB

User's Guide

Default Login Details

LAN IP Address	https://192.168.1.1
User Name	Admin account: admin User account: user
Password	Admin password: 1234 User password: 1234

Version 3.00
Edition 1, 4/2012

ZyXEL

www.zyxel.com

Copyright © 2012
ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guid shows how to connect the EMG5324-D10A and access the Web Configurator. It information on setting up and configuring the EMG5324-D10A.

Contents Overview

User's Guide 15

Introduction 17
Introducing the Web Configurator 23
Tutorials 31

Technical Reference 73

Connection Status and System Info 75
Broadband 81
Wireless 95
Home Networking 121
Routing 145
Quality of Service (QoS) 149
Network Address Translation (NAT) 161
DNS Route 171
Interface Group 175
Firewall 177
MAC Filter 185
Parental Control 187
Certificates 191
VPN 201
VoIP 221
Logs 243
Traffic Status 247
User Account 253
Remote MGMT 255
The SNMP Screen 257
System 259
Time Setting 261
Log Setting 263
Firmware Upgrade 265
Backup/Restore 267
Diagnostic 271
Troubleshooting 273
Wall-mounting Instructions 281

Table of Contents

Contents Overview **3**

Table of Contents **5**

Part I: User's Guide **15**

Chapter 1
Introduction **17**

1.1 Overview 17
1.2 Applications for the Device 17
1.2.1 Internet Access 17
1.2.2 VoIP Features 18
1.2.3 Wireless Connection 18
1.3 The WLAN Button 18
1.4 Ways to Manage the Device 20
1.5 Good Habits for Managing the Device 20
1.6 LEDs (Lights) 20
1.7 The RESET Button 22

Chapter 2
Introducing the Web Configurator **23**

2.1 Overview 23
2.1.1 Accessing the Web Configurator 23
2.2 The Web Configurator Layout 25
2.2.1 Title Bar 25
2.2.2 Main Window 26
2.2.3 Navigation Panel 26

Chapter 3
Tutorials **31**

3.1 Overview 31
3.2 How to Set up a Wireless Network 31
3.2.1 Example Parameters 31
3.2.2 Configuring the AP 32
3.2.3 Configuring the Wireless Client 33
3.3 Setting Up NAT Port Forwarding 38
3.4 How to Make a VoIP Call 39
3.4.1 VoIP Calls With a Registered SIP Account 40

3.5 Using the File Sharing Feature 42
3.5.1 Set Up File Sharing 43
3.5.2 Access Your Shared Files From a Computer 44
3.6 Using the Media Server Feature 44
3.6.1 Configuring the Device 45
3.6.2 Using Windows Media Player 45
3.6.3 Using a Digital Media Adapter 48
3.7 Using the Print Server Feature 50
3.8 Configuring the MAC Address Filter 65
3.9 Configuring Static Route for Routing to Another Network 66
3.10 Configuring QoS Queue and Class Setup 68
3.11 Access the Device Using DDNS 71
3.11.1 Registering a DDNS Account on www.dyndns.org 72
3.11.2 Configuring DDNS on Your Device 72
3.11.3 Testing the DDNS Setting 72

Part II: Technical Reference 73

Chapter 4
Connection Status and System Info 75

4.1 Overview 75
4.2 The Connection Status Screen 75
4.3 The System Info Screen 77

Chapter 5
Broadband 81

5.1 Overview 81
5.1.1 What You Can Do in this Chapter 82
5.1.2 What You Need to Know 82
5.1.3 Before You Begin 84
5.2 The Broadband Screen 84
5.2.1 Add/Edit Internet Connection 85
5.3 The 3G Backup Screen 89
5.4 Technical Reference 91

Chapter 6
Wireless 95

6.1 Overview 95
6.1.1 What You Can Do in this Chapter 95
6.1.2 Wireless Network Overview 95
6.1.3 Before You Begin 97

6.2 The Wireless General Screen 97
6.2.1 No Security 98
6.2.2 Basic (Static WEP/Shared WEP Encryption) 99
6.2.3 More Secure (WPA(2)-PSK) 101
6.2.4 WPA(2) Authentication 102
6.3 The More AP Screen 103
6.3.1 Edit More AP 104
6.4 The WPS Screen 105
6.5 The WMM Screen 107
6.6 Scheduling Screen 108
6.7 The Channel Status Screen 109
6.8 Technical Reference 109
6.8.1 Additional Wireless Terms 110
6.8.2 Wireless Security Overview 110
6.8.3 Signal Problems 112
6.8.4 BSS 113
6.8.5 WiFi Protected Setup (WPS) 113

Chapter 7
Home Networking 121

7.1 Overview 121
7.1.1 What You Can Do in this Chapter 121
7.1.2 What You Need To Know 121
7.2 The LAN Setup Screen 124
7.3 The Static DHCP Screen 125
7.3.1 Before You Begin 125
7.4 The UPnP Screen 127
7.5 The File Sharing Screen 127
7.5.1 Before You Begin 128
7.5.2 Add/Edit File Sharing 129
7.6 The Media Server Screen 130
7.7 The Printer Server Screen 131
7.7.1 Before You Begin 131
7.8 Technical Reference 132
7.9 Installing UPnP in Windows Example 136
7.10 Using UPnP in Windows XP Example 139

Chapter 8
Routing 145

8.1 Overview 145
8.2 Configuring Static Route 146
8.2.1 Add/Edit Static Route 147

Chapter 9
Quality of Service (QoS) 149

9.1 Overview 149
9.1.1 What You Can Do in this Chapter 149
9.1.2 What You Need to Know 149
9.2 The QoS General Screen 150
9.3 The Queue Setup Screen 151
9.3.1 Add/Edit a QoS Queue 152
9.4 The Class Setup Screen 153
9.4.1 Add/Edit QoS Class 155
9.5 The QoS Monitor Screen 158
9.6 QoS Technical Reference 159
9.6.1 IEEE 802.1Q Tag 159
9.6.2 IP Precedence 160
9.6.3 DiffServ 160

Chapter 10
Network Address Translation (NAT) 161

10.1 Overview 161
10.1.1 What You Can Do in this Chapter 161
10.1.2 What You Need To Know 161
10.2 The Port Forwarding Screen 162
10.2.1 The Port Forwarding Screen 163
10.2.2 The Port Forwarding Edit Screen 164
10.3 The DMZ Screen 165
10.4 The Sessions Screen 165
10.5 The Address Mapping Screen 166
10.5.1 Add/Edit Address Mapping Rule 167
10.6 The ALG Screen 168
10.7 Technical Reference 168
10.7.1 NAT Definitions 168
10.7.2 What NAT Does 169
10.7.3 How NAT Works 169

Chapter 11
DNS Route 171

11.1 Overview 171
11.2 The DNS Route Screen 172
11.2.1 Add/Edit DNS Route Edit 172

Chapter 12
Interface Group 175

12.1 Overview 175

12.2 The Interface Group Screen 175
12.2.1 Interface Group Configuration 176

Chapter 13
Firewall 177

13.1 Overview 177
13.1.1 What You Can Do in this Chapter 177
13.1.2 What You Need to Know 178
13.2 The General Screen 178
13.3 The Services Screen 179
13.3.1 Add/Edit a Service 180
13.4 The Access Control Screen 181
13.4.1 Add/Edit an ACL Rule 182
13.5 The DoS Screen 183
13.6 Firewall Technical Reference 183
13.6.1 Guidelines For Enhancing Security With Your Firewall 184
13.6.2 Security Considerations 184

Chapter 14
MAC Filter 185

14.1 Overview 185
14.1.1 What You Need to Know 185
14.2 The MAC Filter Screen 185

Chapter 15
Parental Control 187

15.1 Overview 187
15.2 The Parental Control Screen 187
15.2.1 Add/Edit a Parental Control Rule 188

Chapter 16
Certificates 191

16.1 Overview 191
16.1.1 What You Can Do in this Chapter 191
16.1.2 What You Need to Know 191
16.1.3 Verifying a Certificate 192
16.2 Local Certificates 193
16.3 Trusted CA 195
16.4 Trusted CA Import 195
16.5 View Certificate 196
16.6 VPN Certificates 197
16.6.1 Import Certificate 198

Chapter 17
VPN 201

17.1 Overview 201
17.1.1 What You Can Do in the VPN Screens 201
17.1.2 What You Need to Know About IPSec VPN 201
17.1.3 Before You Begin 203
17.2 VPN Setup Screen 203
17.3 The VPN Edit Screen 205
17.4 Configuring Advanced Settings 208
17.5 Viewing SA Monitor 210
17.6 IPSec VPN Technical Reference 210
17.6.1 IPSec Architecture 211
17.6.2 IPSec and NAT 211
17.6.3 VPN, NAT, and NAT Traversal 212
17.6.4 Encapsulation 213
17.6.5 IKE Phases 214
17.6.6 Negotiation Mode 215
17.6.7 Remote DNS Server 215
17.6.8 ID Type and Content 216
17.6.9 Pre-Shared Key 217
17.6.10 Diffie-Hellman (DH) Key Groups 217
17.6.11 Telecommuter VPN/IPSec Examples 217

Chapter 18
VoIP 221

18.1 Overview 221
18.1.1 What You Can Do in this Chapter 221
18.1.2 What You Need to Know 221
18.1.3 Before You Begin 222
18.2 The SIP Service Provider Screen 223
18.3 The SIP Account Screen 226
18.3.1 Add/Edit SIP Account 227
18.4 Multiple SIP Accounts 229
18.5 Phone Screen 230
18.5.1 Edit Phone Device 230
18.6 The Phone Region Screen 231
18.7 The Call Rule Screen 232
18.8 Technical Reference 233
18.8.1 VoIP 233
18.8.2 SIP 233
18.8.3 Quality of Service (QoS) 238
18.8.4 Phone Services Overview 239

Chapter 19
Logs 243

19.1 Overview 243
19.1.1 What You Can Do in this Chapter 243
19.1.2 What You Need To Know 243
19.2 The System Log Screen 244
19.3 The Phone Log Screen 245
19.4 The VoIP Call History Screen 245

Chapter 20
Traffic Status 247

20.1 Overview 247
20.1.1 What You Can Do in this Chapter 247
20.2 The WAN Status Screen 247
20.3 The LAN Status Screen 248
20.4 The NAT Status Screen 249
20.5 The 3G Backup Status Screen 250
20.6 The VoIP Status Screen 251

Chapter 21
User Account 253

21.1 Overview 253
21.2 The User Account Screen 253

Chapter 22
Remote MGMT 255

22.1 Overview 255
22.1.1 What You Need to Know 255
22.2 The Remote MGMT Screen 256

Chapter 23
The SNMP Screen 257

Chapter 24
System 259

24.1 Overview 259
24.1.1 What You Need to Know 259
24.2 The System Screen 259

Chapter 25
Time Setting 261

25.1 Overview 261
25.2 The Time Setting Screen 261

Chapter 26
Log Setting 263

26.1 Overview 263
26.2 The Log Setting Screen 263

Chapter 27
Firmware Upgrade 265

27.1 Overview 265
27.2 The Firmware Upgrade Screen 265

Chapter 28
Backup/Restore 267

28.1 Overview 267
28.2 The Backup/Restore Screen 267
28.3 The Reboot Screen 269

Chapter 29
Diagnostic 271

29.1 Overview 271
29.2 The Ping/TraceRoute Screen 271
29.3 The DSL Line Screen 272

Chapter 30
Troubleshooting 273

30.1 Overview 273
30.2 Power, Hardware Connections, and LEDs 273
30.3 Device Access and Login 274
30.4 Internet Access 276
30.5 Wireless Internet Access 277
30.6 Phone Calls and VoIP 278
30.7 USB Device Connection 279
30.8 UPnP 279

Chapter 31
Wall-mounting Instructions 281

Appendix A IP Addresses and Subnetting 283

Appendix B Setting Up Your Computer's IP Address 293

Appendix C Pop-up Windows, JavaScript and Java Permissions 323

Appendix D Wireless LANs 333

Appendix E Common Services 353

Appendix F IPv6 357

Appendix G Legal Information 369

Index 373

PART I
User's Guide

1 Introduction

1.1 Overview

The Device is an Ethernet integrated access device (IAD), which provides Voice over IP (VoIP) communication capabilities to allow you to use a traditional analog telephone to make Internet calls. By integrating all of these features, you are provided with ease of installation and high-speed, shared Internet access. The Device is also a complete security solution with a robust firewall based on Stateful Packet Inspection (SPI) technology and Denial of Service (DoS).

When the Device does not have power, only the phone connected to the PHONE port 1 can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.

1.2 Applications for the Device

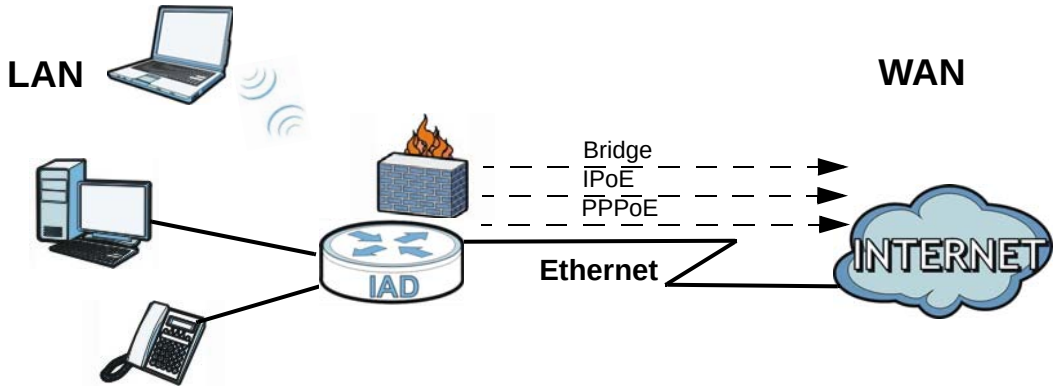
Here are some example uses for which the Device is well suited.

1.2.1 Internet Access

If you have another broadband modem or router available, you can connect the **WAN** port to the it. This way, you can access the Internet via an Ethernet connection and still use the QoS, Firewall and VoIP functions on the Device.

Computers can connect to the Device's LAN ports (or wirelessly).

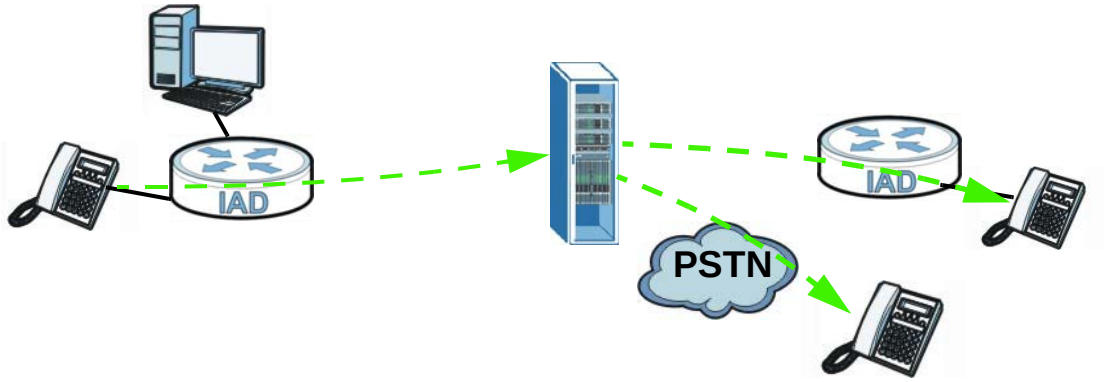
Figure 1 Device's Internet Access Application



1.2.2 VoIP Features

You can register 1 SIP (Session Initiation Protocol) profile (2 accounts for that profile) and use the Device to make and receive VoIP telephone calls:

Figure 2 Device's VoIP Application

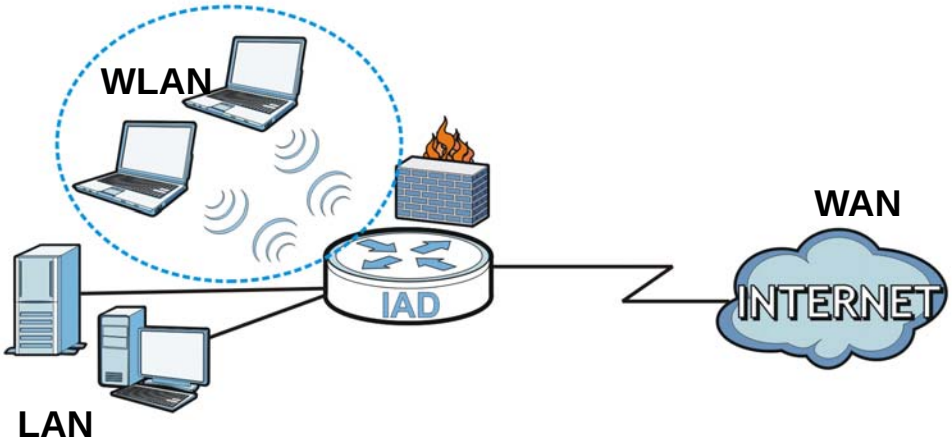


The Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

1.2.3 Wireless Connection

By default, the wireless LAN (WLAN) is enabled on the Device. Once Wireless is enabled, IEEE 802.11b/g/n compliant clients can wirelessly connect to the Device to access network resources. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

Figure 3 Wireless Connection Application



1.3 The WLAN Button

You can use the **WLAN ON/OFF** button on top of the device to turn the wireless LAN on or off. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

Turn the Wireless LAN On or Off

1 Make sure the **POWER** LED is on (not blinking).

2 Press the **WLAN ON/OFF** button for one second and release it. The **WLAN / WPS** LED should change from on to off or vice versa.

Activate WPS

1 Make sure the **POWER** LED is on (not blinking).

2 Press the **WLAN ON/OFF** button for more than five seconds and release it. Press the WPS button on another WPS -enabled device within range of the Device. The **WLAN / WPS** LED should flash while the Device sets up a WPS connection with the wireless device.

Note: You must activate WPS in the Device and in another wireless device within two minutes of each other. See Chapter 6 on page 113 for more information.

1.4 Ways to Manage the Device

Use any of the following methods to manage the Device.

- Web Configurator. This is recommended for everyday management of the Device using a (supported) web browser.
- FTP for firmware upgrades and configuration backup/restore.

1.5 Good Habits for Managing the Device

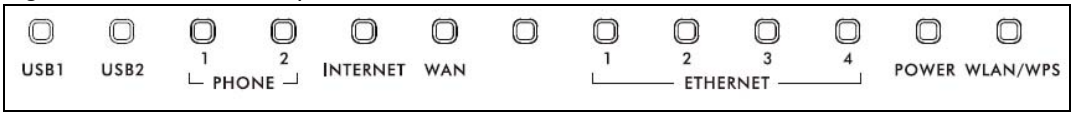
Do the following things regularly to make the Device more secure and to manage the Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password to access the Web Configurator, you will have to reset the Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Device. You could simply restore your last configuration. Keep in mind that backing up a configuration file will not back up passwords used to set up PPPoE and VoIP. Write down any information your ISP provides you.

1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 4 LEDs on the Top of the Device



None of the LEDs are on if the Device is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
USB1-2	Green	On	The Device recognizes a USB connection but there is no traffic.
		Blinking	The Device is sending/receiving data to /from the USB device connected to it.
	Off		The Device does not detect a USB connection.

Table 1 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
PHONE1-2	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
	Off		The phone port does not have a SIP account registered.
INTERNET	Green	On	The Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used).
		Blinking	The Device is sending or receiving IP traffic.
		Off	The Device does not have an IP connection.
	Red	On	The Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
WAN	Green	On	This light applies when the Device is in Ethernet WAN mode. The Device has an Ethernet connection with a device on the WAN.
		Blinking	The Device is sending or receiving data to/from the Ethernet WAN.
		Off	The Device does not have an Ethernet connection with the WAN.
ETHERNET1-4	Green (Giga Ethernet)	On	The Device has a successful 1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Device is sending or receiving data to/from the LAN at 1000 Mbps.
	Orange (Fast Ethernet)	On	The Device has a successful 10/100 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Device is sending or receiving data to/from the LAN at 10/100 Mbps.
	Off		The Device does not have an Ethernet connection with the LAN.
POWER	Green	On	The Device is receiving power and ready for use.
		Blinking	The Device is self-testing.
	Red	On	The Device detected an error while self-testing, or there is a device malfunction.
	Off		The Device is not receiving power.
WLAN/WPS	Green	On	The wireless network is activated and is operating in IEEE 802.11 “b”, “g” or “n” mode.
		Blinking	The Device is communicating with other wireless clients.
	Orange	On	The WPS is configured.
		Blinking	The Device is setting up a WPS connection.
	Off		The wireless network is not activated.

Refer to the Quick Start Guide for information on hardware connections.

1.7 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the passwords will be reset to the defaults.

1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for 5 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

2

Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See Appendix C on page 323 if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

1. Make sure your Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. A password screen displays. Type “admin” as the default Username and “1234” as the default password to access the device’s Web Configurator. Click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 5 Password Screen

Note: For security reasons, the Device automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

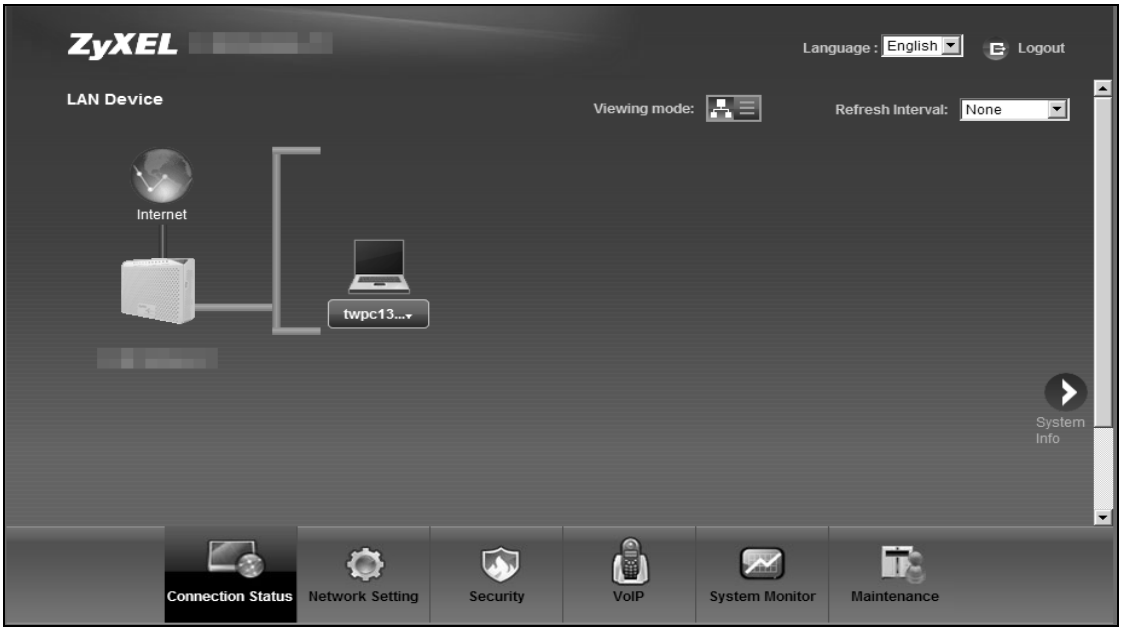
5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Skip** to proceed to the main menu if you do not want to change the password now.

Figure 6 Change Password Screen

ZyXEL
Change Password
It is highly recommended to setup a new password instead of using the default one for security concern.
New Password:
Verify New Password:
Skip
Apply

6 The **Connection Status** screen appears.

Figure 7 Connection Status

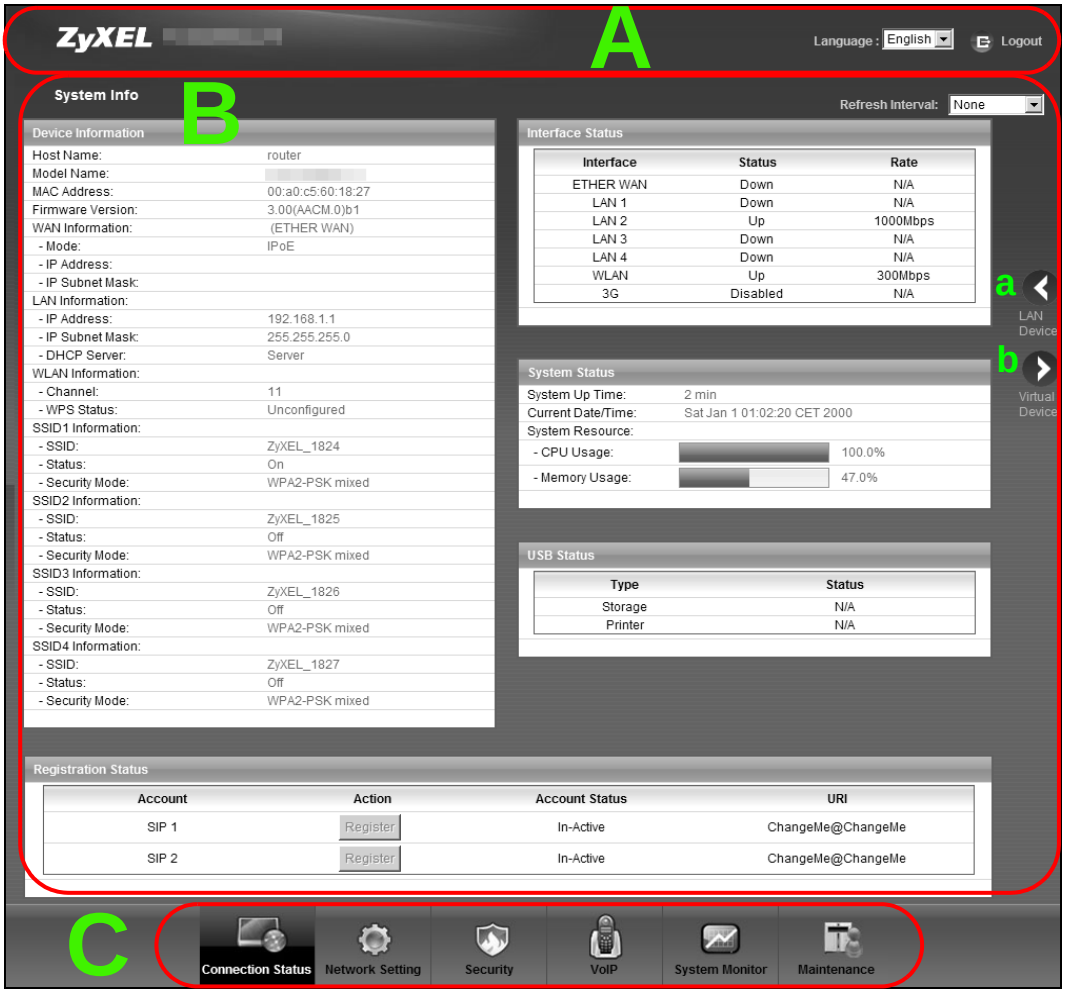


7 Click **System Info** to display the **System Info** screen, where you can view the Device's interface and system information.

2.2 The Web Configurator Layout

Click **Connection Status > System Info** to show the following screen.

Figure 8 Web Configurator Layout



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - main window
- **C** - navigation panel

2.2.1 Title Bar

The title bar shows the following icon in the upper right corner.

Click this icon to log out of the web configurator.

2.2.2 Main Window

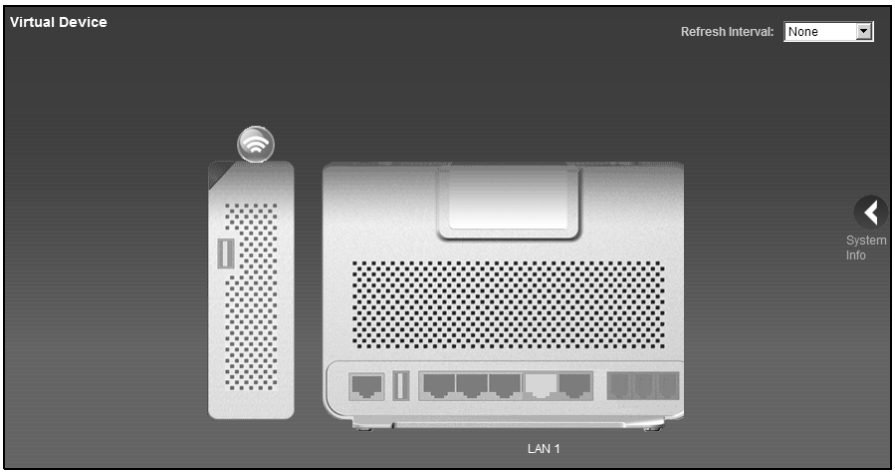
The main window displays information and configuration fields. It is discussed in the rest of this document.

After you click **System Info** on the **Connection Status** screen, the **System Info** screen is displayed. See Chapter 4 on page 77 for more information about the **System Info** screen.

If you click **LAN Device** on the **System Info** screen (**a** in Figure 8 on page 25), the **Connection Status** screen appears. See Chapter 4 on page 75 for more information about the **Connection Status** screen.

If you click **Virtual Device** on the **System Info** screen (**b** in Figure 8 on page 25), a visual graphic appears, showing the connection status of the Device's ports. The connected ports are in color and disconnected ports are gray.

Figure 9 Virtual Device



2.2.3 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Device features. The following table describes each menu item.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the Device and computers/ devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and modify your WAN interface. You can also configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	3G Backup	Use this screen to configure the 3G WAN connection.

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Wireless	General	Use this screen to turn the wireless connection on or off, specify the SSID(s) and configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the Device.
	WPS	Use this screen to use WPS (Wi-Fi Protected Setup) to establish a wireless connection.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	Scheduling	Use this screen to configure when the Device enables or disables the wireless LAN.
	Channel Status	Use this screen to scan wireless LAN channel noises and view the results.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to enable the UPnP function.
	File Sharing	Use this screen to enable file sharing via the Device.
	Media Server	Use this screen to enable or disable the sharing of media files.
	Printer Server	Use this screen to enable or disable sharing of a USB printer via your Device.
Static Route	Static Route	Use this screen to view and set up static routes on the Device.
DNS Route	DNS Route	Use this screen to view and configure DNS routes.
QoS	General	Use this screen to enable QoS and decide allowable bandwidth using QoS.
	Queue Setup	Use this screen to configure QoS queue assignment.
	Class Setup	Use this screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
	Monitor	Use this screen to view each queue's statistics.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Sessions	Use this screen to limit the number of NAT sessions a single client can establish.
	Address Mapping	Use this screen to change your Device's address mapping settings.
	ALG	Use this screen to enable or disable SIP ALG.
Dynamic DNS	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Interface Group	Interface Group	Use this screen to map a port to a PVC or bridge group.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	Use this screen to set the default action to take on outgoing network traffic.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
MAC Filter	MAC Filter	Use this screen to allow specific devices to access the Device.
Parental Control	Parental Control	Use this screen to define time periods and days during which the Device performs parental control and/or block web sites with the specific URL.
Certificates	Local Certificates	Use this screen to generate and export self-signed certificates or certification requests and import the Device's CA-signed certificates.
	Trusted CA	Use this screen to save CA certificates to the Device.
	VPN Certificates	Use this screen to import certificates and privates keys for VPN.
VPN	Setup	Use this screen to manage VPN settings.
	Monitor	Use this screen to view the active VPN tunnel's status.
VoIP		
SIP	SIP Service Provider	Use this screen to configure your Device's Voice over IP settings.
	SIP Account	Use this screen to set up information about your SIP account and configure audio settings such as volume levels for the phones connected to the Device.
Phone	Phone Device	Use this screen to set which phone ports use which SIP accounts.
	Region	Use this screen to select your location.
Call Rule	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
FXO	FXO Device	Use this screen to set up the PSTN line you use to make regular phone calls.
System Monitor		
Log	System Log	Use this screen to view the Device's system logs.
	Phone Log	Use this screen to view the Device's phone logs.
	VoIP Call History	Use this screen to view the Device's VoIP call history.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Device.
	NAT	Use this screen to view the status of NAT sessions on the Device.
	3G Backup	Use this screen to view the status of 3G Backup on the Device.
VoIP Status	VoIP Status	Use this screen to view the SIP, phone, and call status of the Device.
Maintenance		
Users Account	Users Account	Use this screen to configure the passwords your user accounts.
Remote MGMT	Remote MGMT	Use this screen to enable specific traffic directions for network services.
SNMP	SNMP	Use this screen to configure through which interface(s) and from which IP address(es) users can use SNMP to manage the Device.
System	System	Use this screen to configure the Device's name, domain name, management inactivity time-out.
Time Setting	Time Setting	Use this screen to change your Device's time and date.
Log Setting	Log Setting	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Device.

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Backup/ Restore	Backup/Restore	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Device without turning the power off.
Diagnostic	Ping/TraceRoute	Use this screen to test the connections to other devices.
Auto Provision	Auto Provision	Use this screen to enable and configure the Device's auto-provisioning feature.

3

Tutorials

3.1 Overview

This chapter contains the following tutorials:

- How to Set up a Wireless Network
- Setting Up NAT Port Forwarding
- How to Make a VoIP Call
- Using the File Sharing Feature
- Using the Media Server Feature
- Using the Print Server Feature
- Configuring the MAC Address Filter
- Configuring Static Route for Routing to Another Network
- Configuring QoS Queue and Class Setup
- Access the Device Using DDNS

3.2 How to Set up a Wireless Network

This section gives you examples of how to set up an access point and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through the Device wirelessly.

3.2.1 Example Parameters

SSID	SSID_Example3
802.11 mode	802.11b/g
Channel	auto
Security	WPA-PSK (Pre-Shared Key: 12MyWPAPSKpresharedkey34)

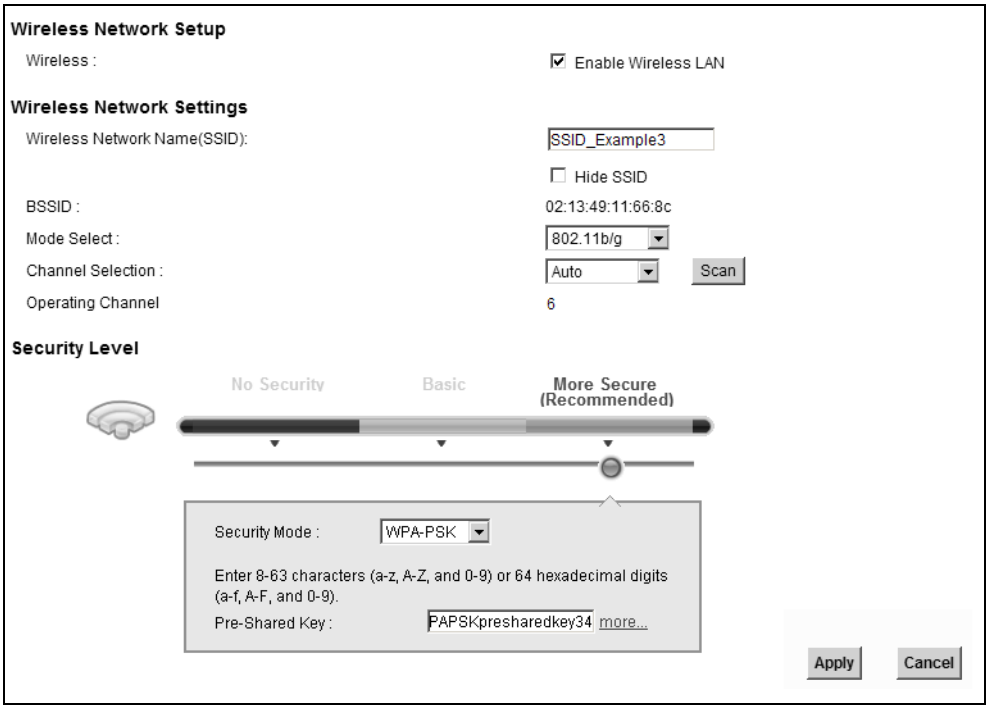
An access point (AP) or wireless router is referred to as the “AP” and a computer with a wireless network card or USB adapter is referred to as the “wireless client” here.

We use the M-302 utility screens as the wireless client example. The screens may vary for different models.

3.2.2 Configuring the AP

Follow the steps below to configure the wireless settings on your AP.

1 Open the **Network Setting > Wireless > General** screen in the AP's web configurator.



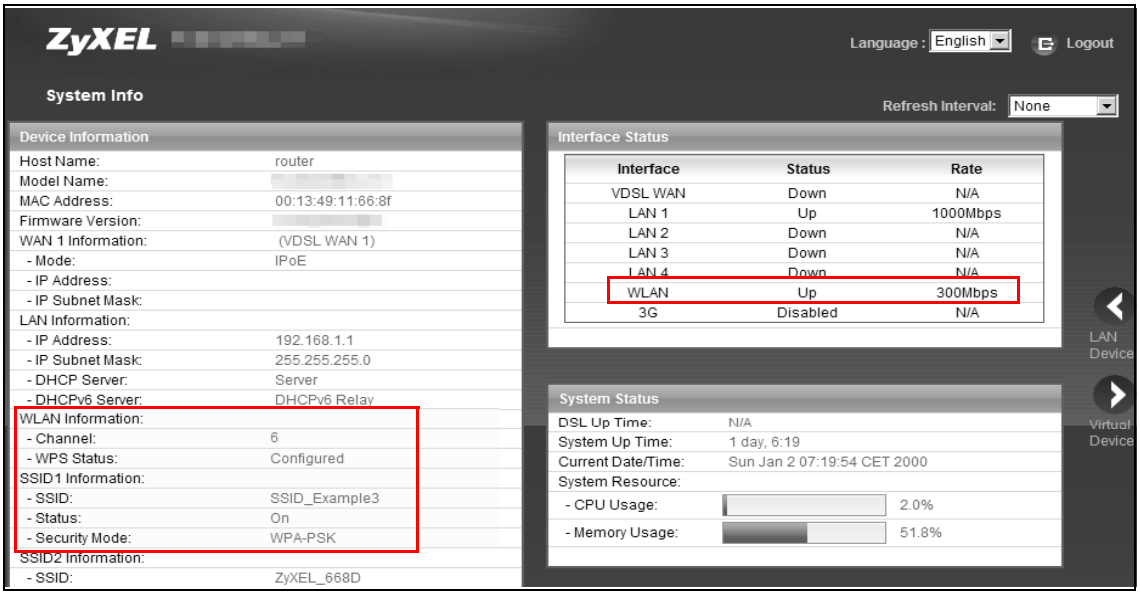
2 Make sure **Enable Wireless LAN** is selected.

3 Enter "SSID_Example3" as the SSID and select **Auto** in the **Channel Selection** field to have the device search for an available channel.

4 Select **802.11b/g** in the **Mode Select** field.

5 Select **More Secure** as your security level and set security mode to **WPA-PSK** and enter "12MyWPAPSKpresharedkey34" in the **Pre-Shared Key** field. Click **Apply**.

6 Click **Connection Status > System Info**.Verify your wireless and wireless security settings under **Device Information** and check if the **WLAN** connection is up under **Interface Status**.



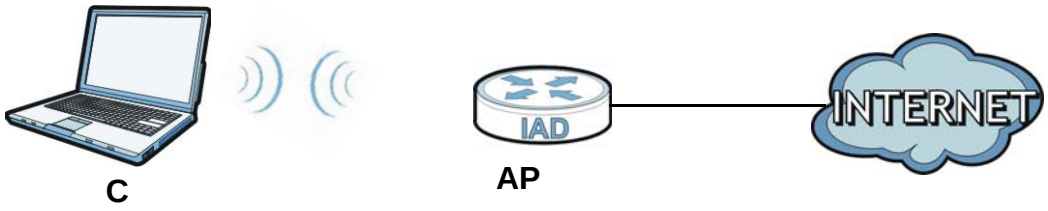
This finishes the configuration of the AP.

3.2.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

3.2.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.



There are three ways to connect the client to an access point.

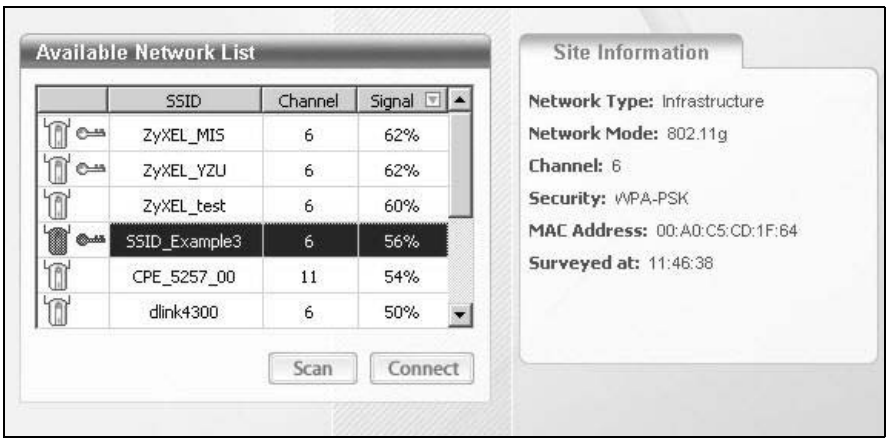
- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access

point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is “SSID_Example3” and the pre-shared key is “12MyWPAPSKpresharedkey34”.

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

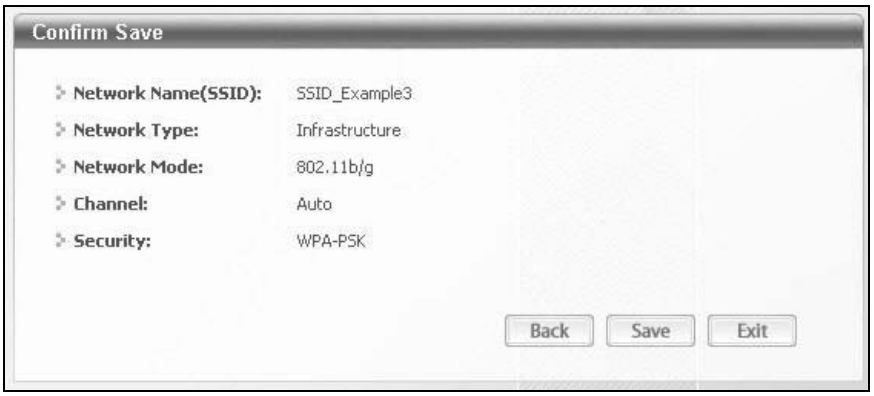


2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.

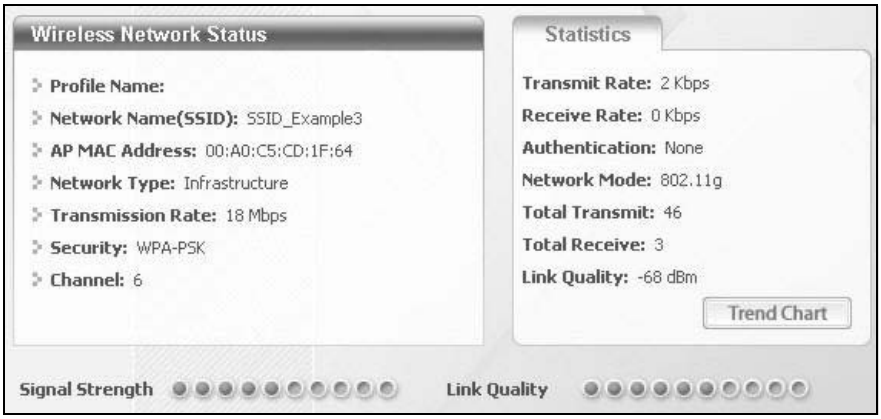
3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.



5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.



6 Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

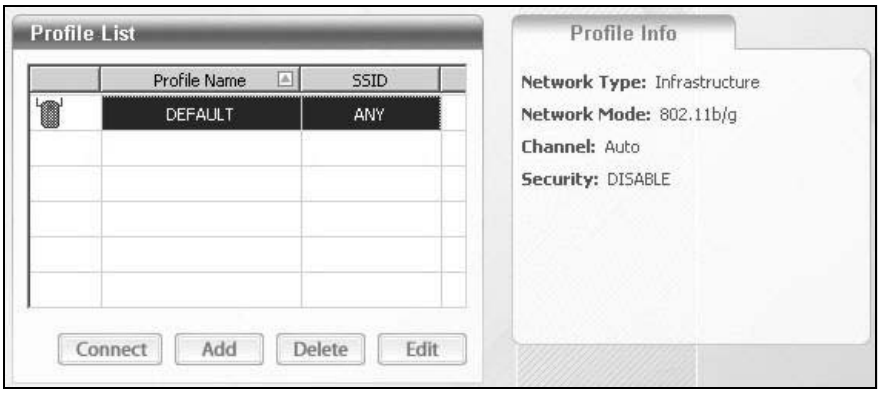
If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

3.2.3.2 Creating and Using a Profile

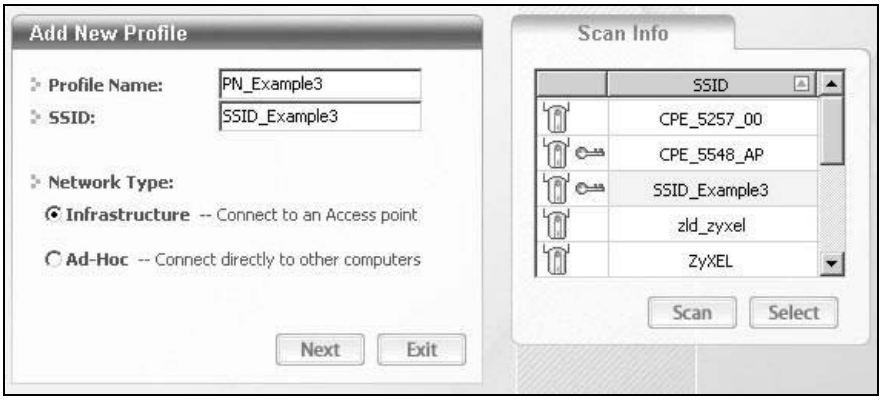
A profile lets you easily connect to the same wireless network again later. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an AP configured for WPA-PSK security. In this example, the SSID is “SSID_Example3”, the profile name is “PN_Example3” and the pre-shared key is “”. You have chosen the profile name “PN_Example3”.

1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

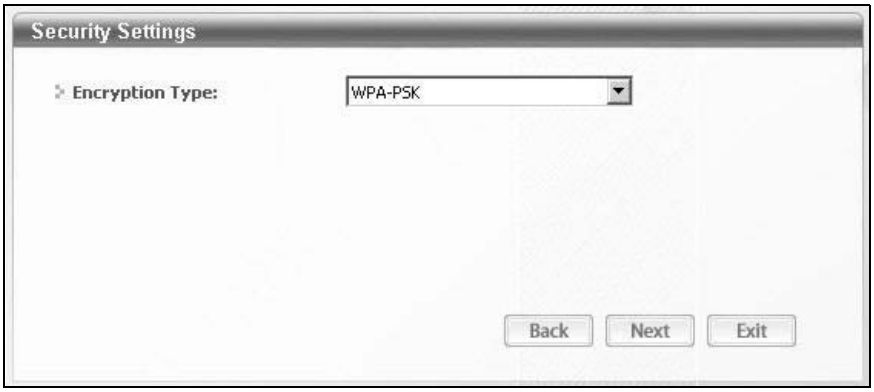


2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, and displays them in the **Scan Info** box. Click **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

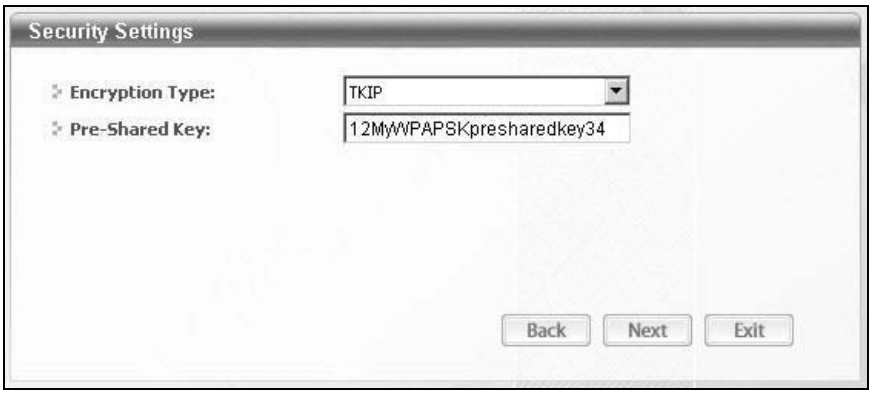


3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

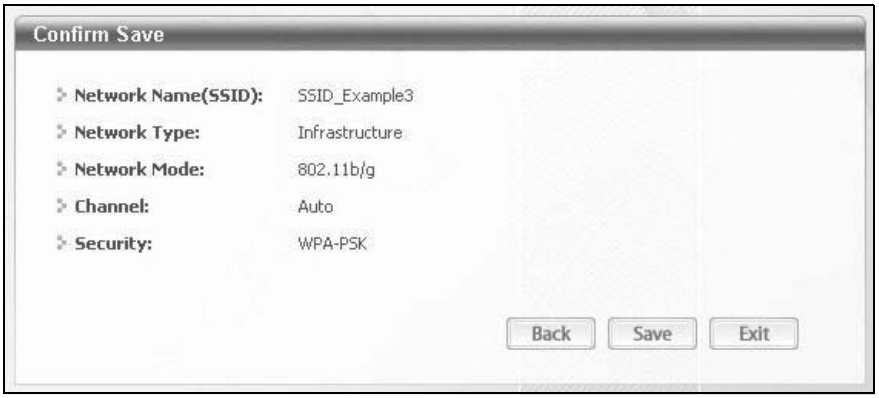


5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.



6 In the next screen, leave both boxes selected.

7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.



8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

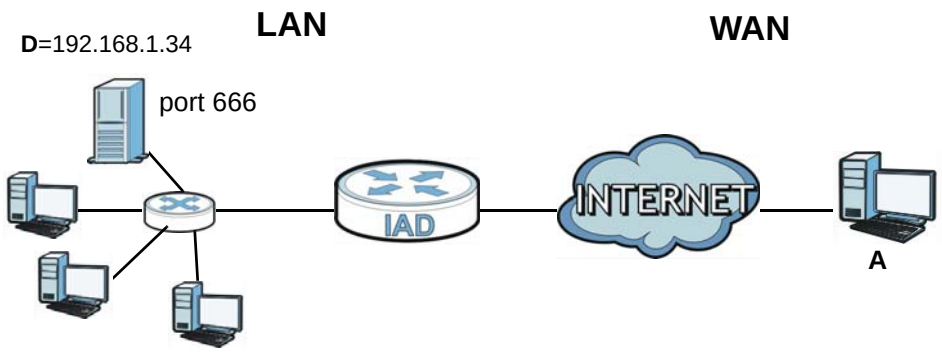
9 When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

10 Open your Internet browser, enter http://www.zyxel.com or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

11 If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

3.3 Setting Up NAT Port Forwarding

In this tutorial, you manage the Doom server on a computer behind the Device. In order for players on the Internet (like **A** in the figure below) to communicate with the Doom server, you need to configure the port settings and IP address on the Device. Traffic should be forwarded to the port 666 of the Doom server computer which has an IP address of 192.168.1.34.

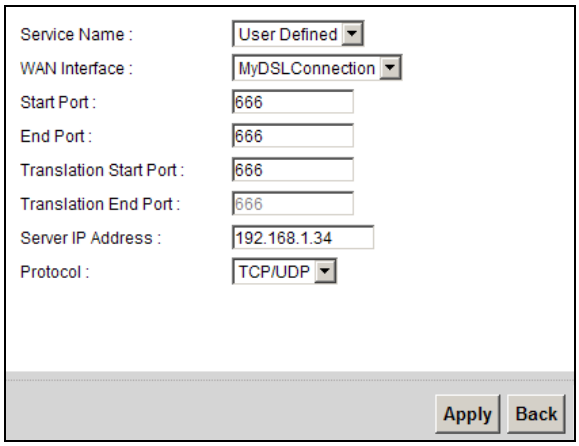


You may set up the port settings by configuring the port settings for the Doom server computer (see Chapter 10 on page 162 for more information).

1 Click **Network Setting** > **NAT** > **Port Forwarding**. Click **Add new rule**.

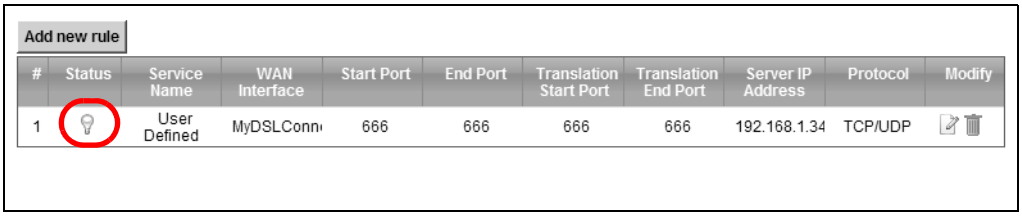
2 Enter the following values:

Service Name	Select **User Defined**.
WAN Interface	Select the WAN interface through which the Doom service is forwarded. This is the default interface for this example, which is **MyDSLConnection**.
Start/End Ports	**666**
Translation Start/End Ports	**666**
Server IP Address	Enter the IP address of the Doom server. This is **192.168.1.34** for this example.
Protocol	Select **TCP/UDP**. This should be the protocol supported by the Doom server.



3 Click **Apply**.

4 The port forwarding settings you configured should appear in the table. Make sure the bulb in **Status** is the color yellow, meaning it is activated. Click **Apply** to have the Device start forwarding port 666 traffic to the computer with IP address 192.168.1.34.


Add new rule
Status Service Name WAN Interface Start Port End Port Translation Start Port Translation End Port Server IP Address Protocol Modify
1 User Defined MyDSLConn 666 666 666 666 192.168.1.34 TCP/UDP

Players on the Internet then can have access to your Doom server.

3.4 How to Make a VoIP Call

You can register a SIP account with the SIP server and make voice calls over the Internet to another VoIP device.

The following parameters are used in this example:

SIP Service Provider Name	ServiceProvider1
SIP Server Address	sip.example.com
REGISTER Server Address	registersip.example.com
SIP Service Domain	sip.example.com
SIP Account Number	12345678
Username	ChangeMe
Password	ThisIsMySIP

3.4.1 VoIP Calls With a Registered SIP Account

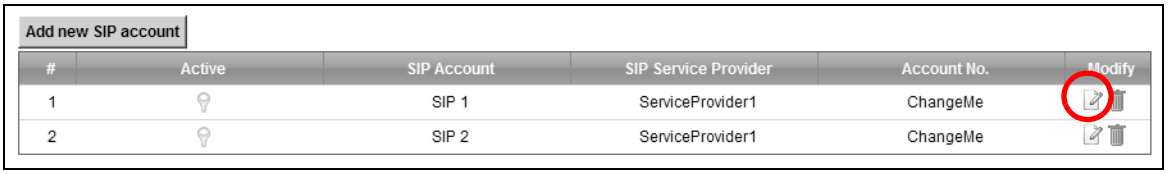
To use a registered SIP account, you should configure the SIP service provider and applied for a SIP account.

3.4.1.1 SIP Service Provider Configuration

Follow the steps below to configure your SIP service provider.

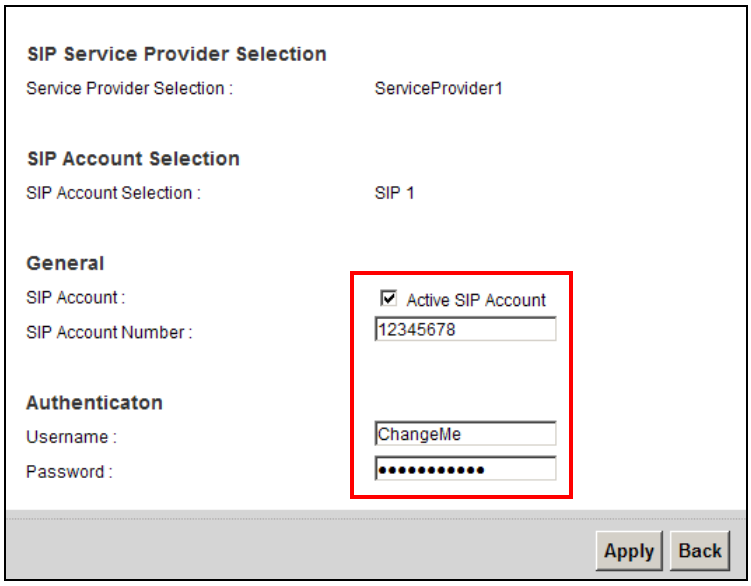
1. Make sure your Device is connected to the Internet.
2. Open the web configurator.
3. Click **VoIP > SIP** to open the **SIP Service Provider** screen. Select **ChangeMe** from the **Service Provider Selection** drop-down list box.
4. Select the **Enable** check box of **SIP Service Provider** and enter **ServiceProvider1** as the **SIP Service Provider Name**. Enter the **SIP Server Address**, **REGISTER Server Address**, and **SIP Service Domain** provided by your ISP accordingly. Click **Apply**.

5 Go to the **SIP Account** screen, click the **Edit** icon of **SIP 1**.


Add new SIP account
Active SIP Account SIP Service Provider Account No. Modify
1 SIP 1 ServiceProvider1 ChangeMe
2 SIP 2 ServiceProvider1 ChangeMe

6 Select the **Active SIP Account** check box, then enter the **SIP Account Number**, **Username**, and **Password**. Leave other settings as default.

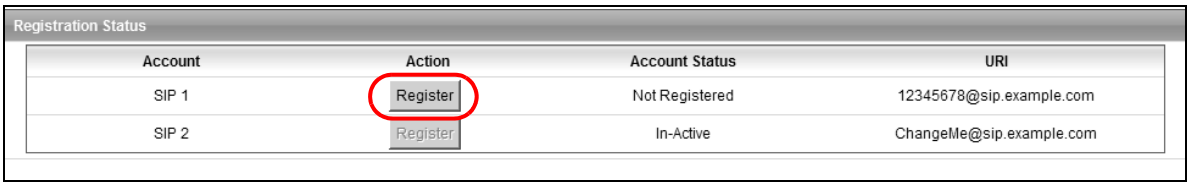
7 Click **Apply** to save your settings.



3.4.1.2 SIP Account Registration

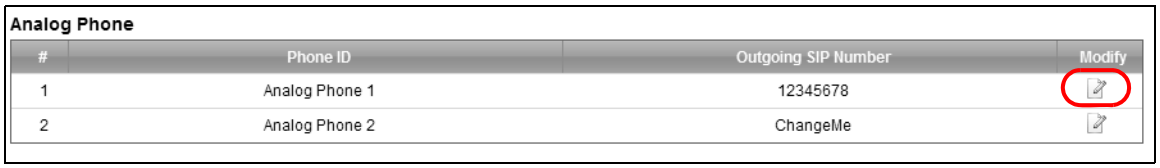
Follow the steps below to register and activate your SIP account.

1 Click **Connection Status > System Info** to check if your SIP account has been registered successfully. If the status is **Not Registered**, check your Internet connection and click **Register** to register your SIP account.


Registration Status
Account Action Account Status URI
SIP 1 Register Not Registered 12345678@sip.example.com
SIP 2 Register In-Active ChangeMe@sip.example.com

3.4.1.3 Analog Phone Configuration

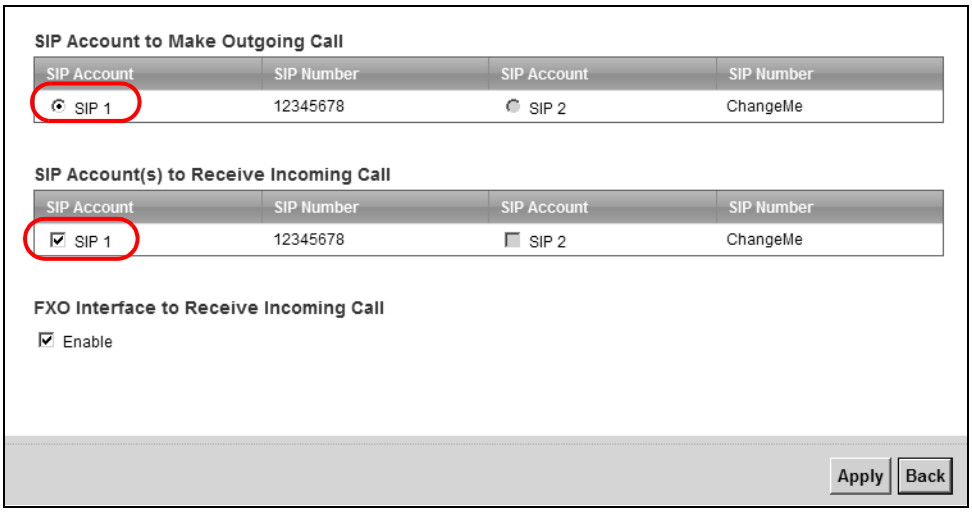
1 Click **VoIP > Phone** to open the **Phone Device** screen. Click the **Edit** icon next to **Analog Phone 1** to configure the first phone port.



2 Select **SIP 1** from the **SIP Account** in the **SIP Account to Make Outgoing Call** section to have the phone (connected to the first phone port) use the registered SIP 1 account to make outgoing calls.

3 Select the **SIP 1** check box in the **SIP Account(s) to Receive Incoming Call** section to have the phone (connected to the first phone port) receive phone calls for the SIP 3 account.

4 Click **Apply** to save your changes.


SIP Account to Make Outgoing Call
SIP Account SIP Number SIP Account SIP Number
SIP 1 12345678 SIP 2 ChangeMe
SIP Account(s) to Receive Incoming Call
SIP Account SIP Number SIP Account SIP Number
SIP 1 12345678 SIP 2 ChangeMe
FXO Interface to Receive Incoming Call
Enable
Apply
Back

3.4.1.4 Making a VoIP Call

1 Make sure you connect a telephone to the first phone port on the Device.

2 Make sure the Device is on and connected to the Internet.

3 Pick up the phone receiver.

4 Dial the VoIP phone number you want to call.

3.5 Using the File Sharing Feature

In this section you can:

- Set up file sharing of your USB device from the Device

- Access the shared files of your USB device from a computer

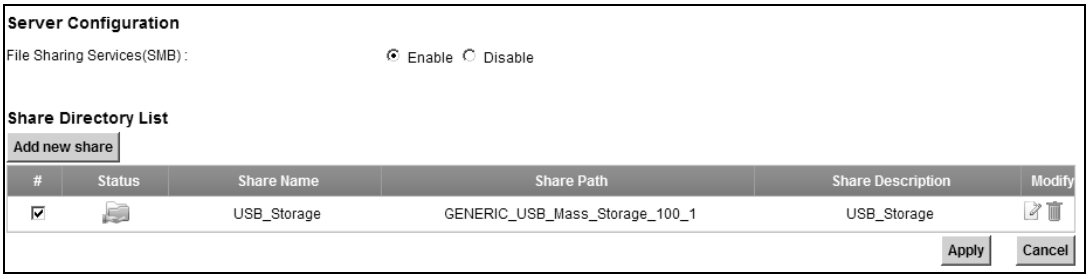
3.5.1 Set Up File Sharing

To set up file sharing you need to connect your USB device, enable file sharing and set up your share(s).

3.5.1.1 Activate File Sharing

1. Connect your USB device to one of the USB ports at the back panel of the Device.

2. Click **Network Setting > Home Networking > File Sharing**. Select **Enable** and click **Apply** to activate the file sharing function. The Device automatically adds your USB device to the **Share Directory List**.

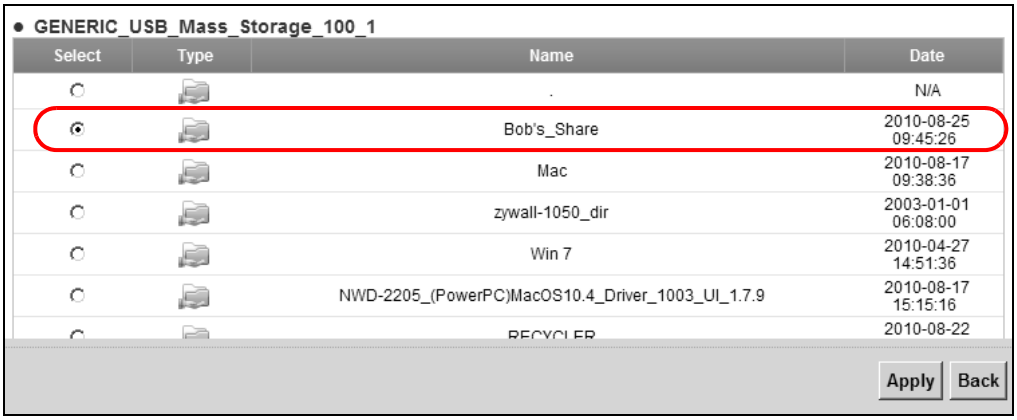


3.5.1.2 Set up File Sharing on Your Device

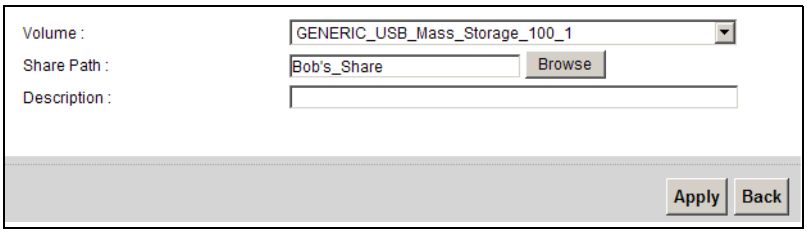
You also need to set up file sharing on your Device in order to share files.

1. Click **Add new share** in the **File Sharing** screen to configure a new share. Select your USB device from the **Volume** drop-down list box.

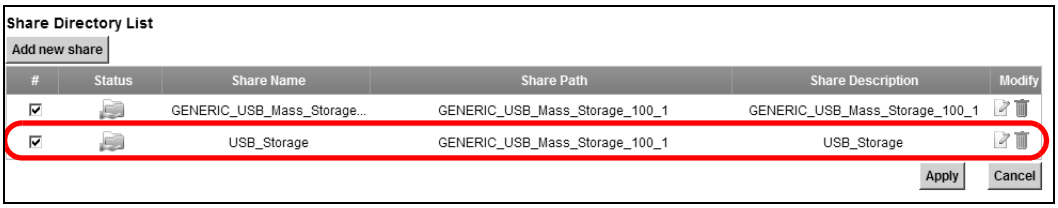
2. Click **Browse** to browse through all the files on your USB device. Select the folder that you want to add as a share. In this example, select **Bob's_Share**. Click **Apply**.



3 You can add a description for the share or leave it blank. The **Add Share Directory** screen should look like the following.Click **Apply** to finish.



4 This sets up the file sharing server. You can see the USB storage device listed in the table below.



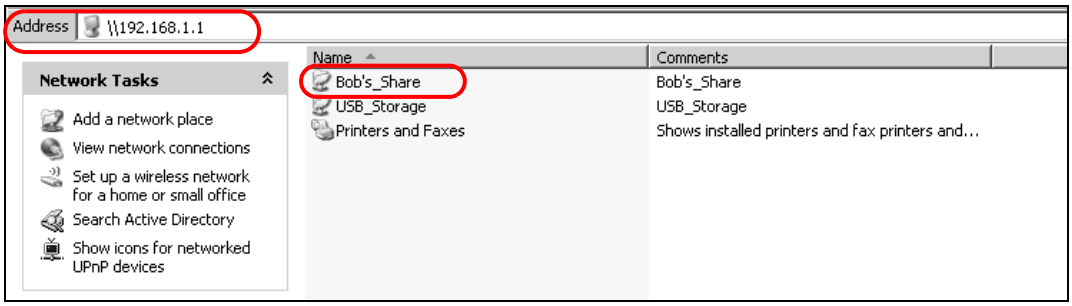
3.5.2 Access Your Shared Files From a Computer

You can use Windows Explorer to access the file storage devices connected to the Device.

Note: The examples in this User's Guide show you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Open Windows Explorer to access Bob's Share using Windows Explorer browser.

In Windows Explorer's Address bar type a double backslash "\\" followed by the IP address of the Device (the default IP address of the Device is 192.168.1.1) and press [ENTER]. The share folder **Bob's_Share** is available.



Once you access **Bob's_Share** via your Device, you do not have to relogin unless you restart your computer.

3.6 Using the Media Server Feature

Use the media server feature to play files on a computer or on your television (using DMA-2500).

This section shows you how the media server feature works using the following media clients:

- Microsoft (MS) Windows Media Player

  Media Server works with Windows Vista and Windows 7. Make sure your computer is able to play media files (music, videos and pictures).
- ZyXEL DMA-2500, a digital media adapter

  You need to set up the DMA-2500 to work with your television (TV). Refer to the DMA-2500 Quick Start Guide for the correct hardware connections.

Before you begin, connect the USB storage device containing the media files you want to play to the USB port of your Device.

3.6.1 Configuring the Device

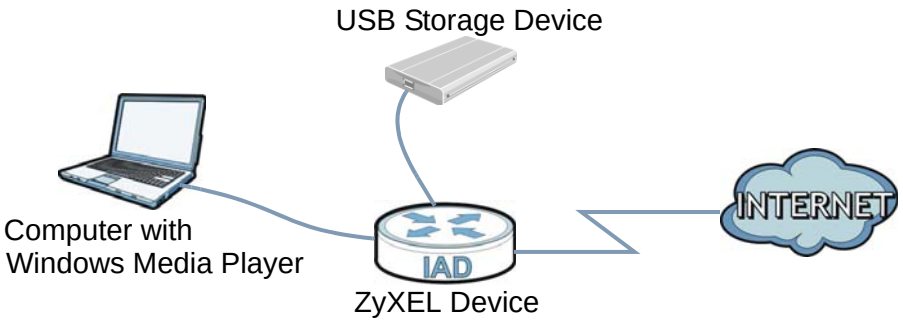
Note: The Media Server feature is enabled by default.

To use your Device as a media server, click **Network Setting > Home Networking > Media Server.**

Check **Enable Media Server** and click **Apply**. This enables DLNA-compliant media clients to play the video, music and image files in your USB storage device.

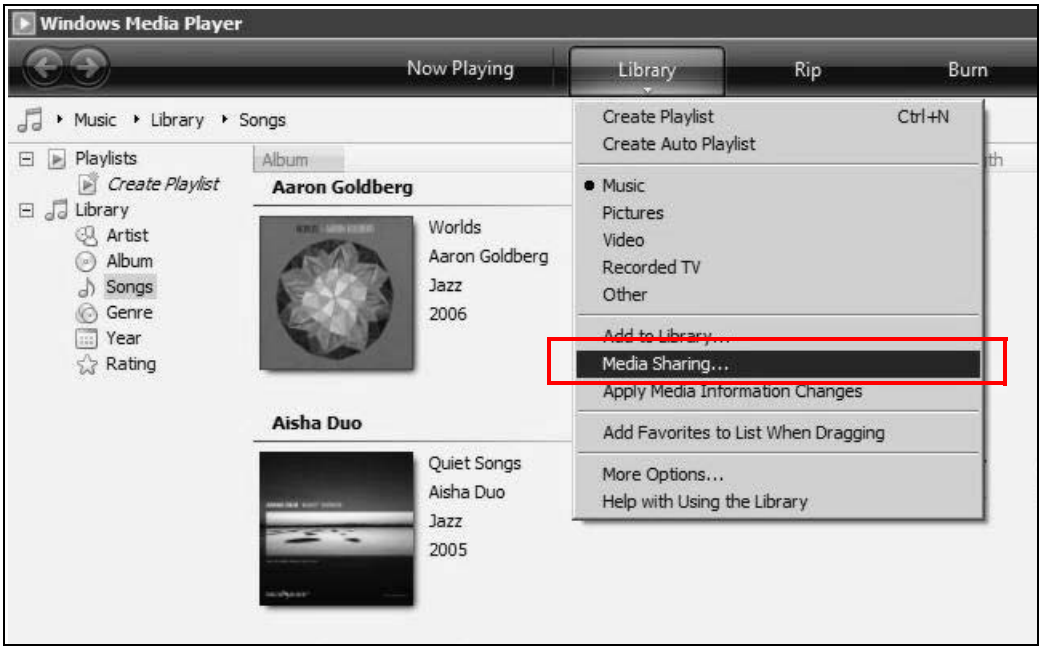
3.6.2 Using Windows Media Player

This section shows you how to play the media files on the USB storage device connected to your Device using Windows Media Player.

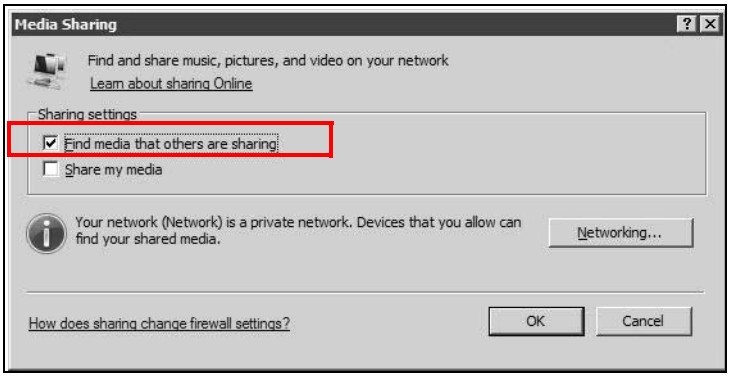


Windows Vista

1 Open Windows Media Player and click **Library > Media Sharing** as follows.



2 Check **Find media that others are sharing** in the following screen and click **OK**.

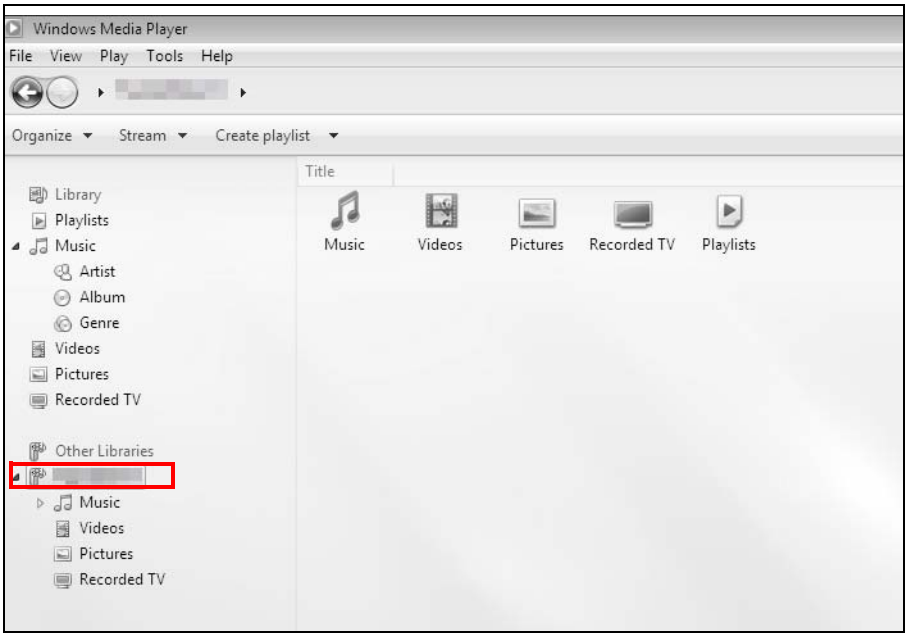

Media Sharing
Find and share music, pictures, and video on your network
Learn about sharing Online
Sharing settings
Find media that others are sharing
Share my media
Your network (Network) is a private network. Devices that you allow can find your shared media.
Networking...
How does sharing change firewall settings?
OK
Cancel

3 In the **Library** screen, check the left panel. The Windows Media Player should detect the Device.

The Device displays as a playlist. Clicking on the category icons in the right panel shows you the media files in the USB storage device attached to your Device.

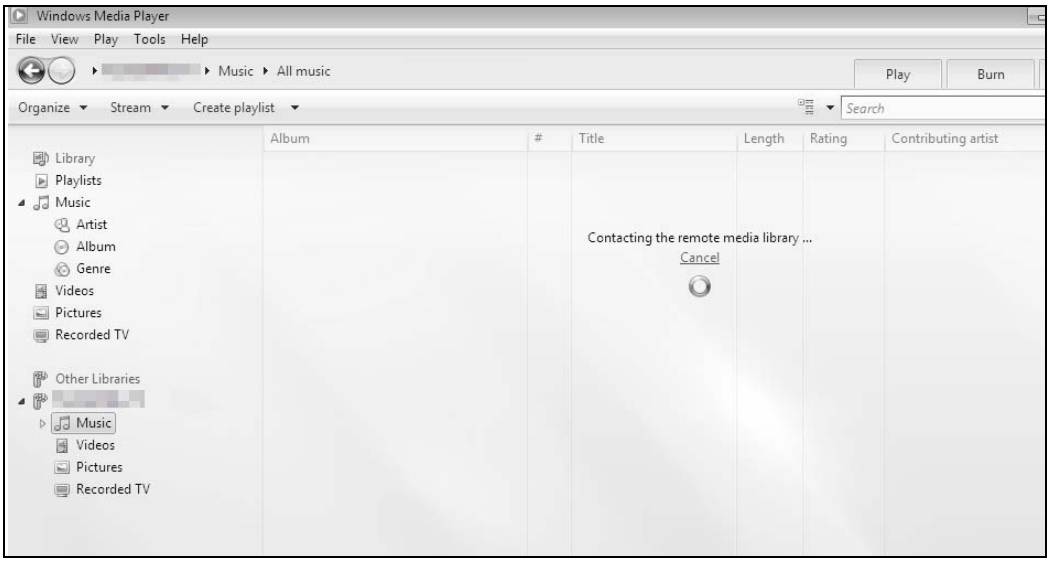
Windows 7

1 Open Windows Media Player. It should automatically detect the Device.

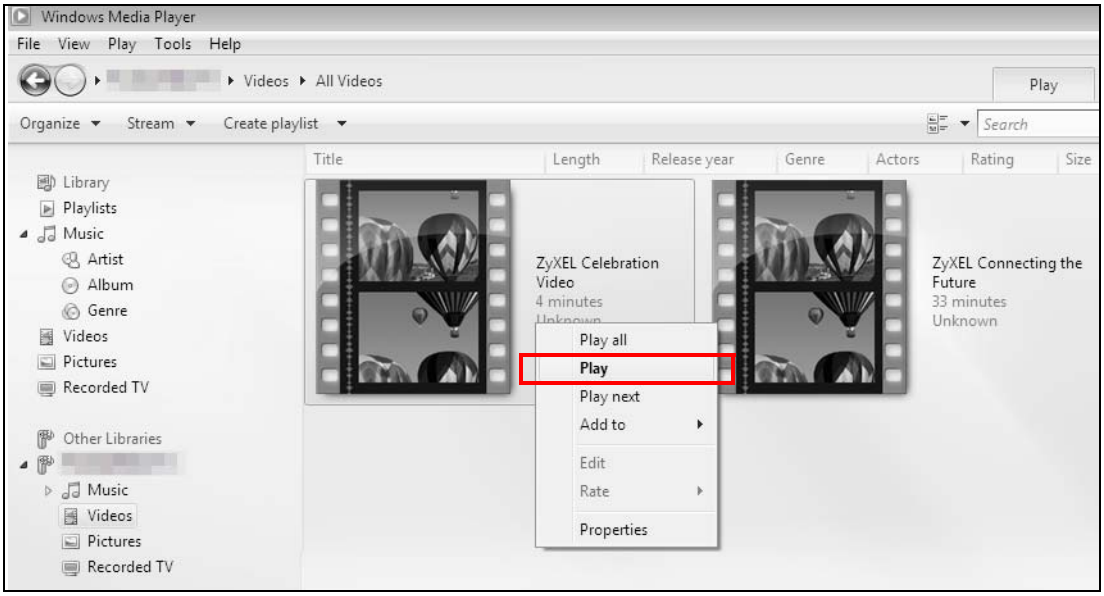


If you cannot see the Device in the left panel as shown above, right-click **Other Libraries > Refresh Other Libraries**.

2 Select a category in the left panel and wait for Windows Media Player to connect to the Device.



3 In the right panel, you should see a list of files available in the USB storage device.

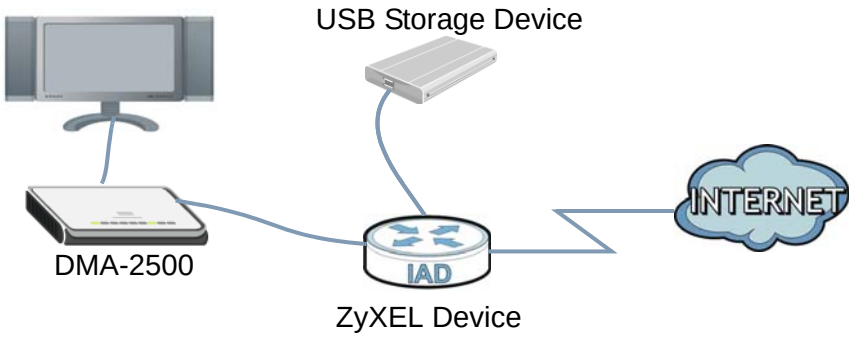


3.6.3 Using a Digital Media Adapter

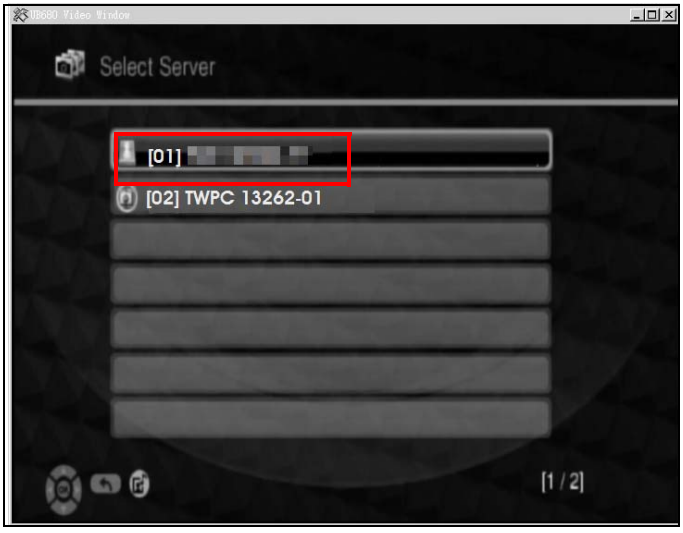
This section shows you how you can use the Device with a ZyXEL DMA-2500 to play media files stored in the USB storage device in your TV screen.

Note: For this tutorial, your DMA-2500 should already be set up with the TV according to the instructions in the DMA-2500 Quick Start Guide.

1 Connect the DMA-2500 to an available LAN port in your Device.



2 Turn on the TV and wait for the DMA-2500 **Home** screen to appear. Using the remote control, go to **MyMedia** to open the following screen. Select the Device as your media server.



3 The screen shows you the list of available media files in the USB storage device. Select the file you want to open and push the **Play** button in the remote control.

3.7 Using the Print Server Feature

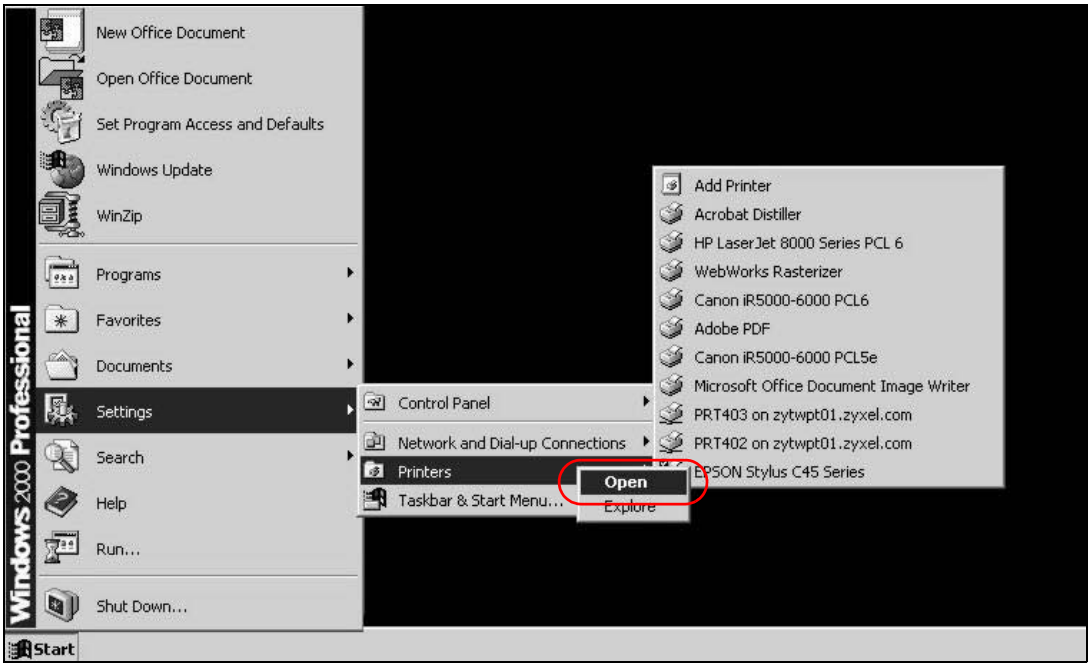
In this section you can:

- Configure a TCP/IP Printer Port
- Add a New Printer Using Windows
- Add a New Printer Using Macintosh OS X

Configure a TCP/IP Printer Port

This example shows how you can configure a TCP/IP printer port. This example is done using the Windows 2000 Professional operating system. Some menu items may look different on your operating system. The TCP/IP port must be configured with the IP address of the Device and must use the RAW protocol to communicate with the printer. Consult your operating systems documentation for instructions on how to do this or follow the instructions below if you have a Windows 2000/XP operating system.

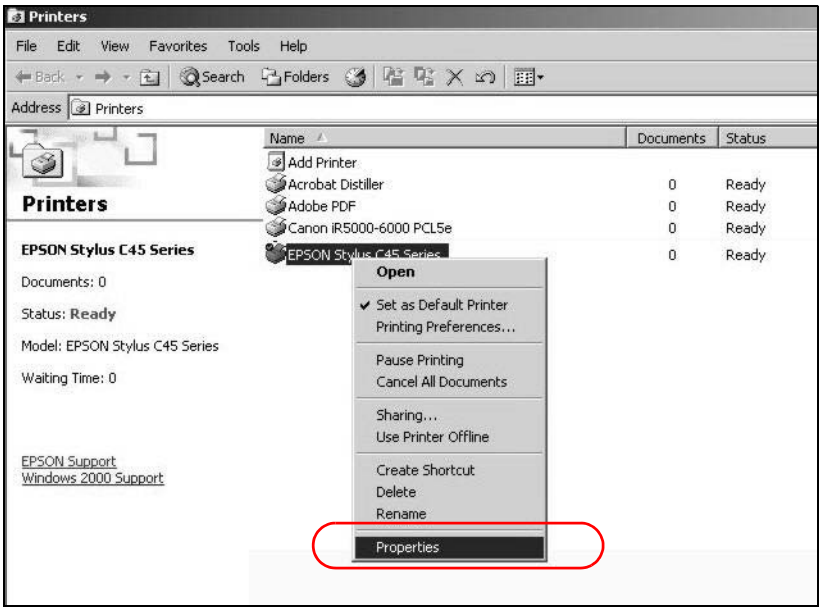
1 Click **Start** > **Settings**, then right click on **Printers** and select **Open**.



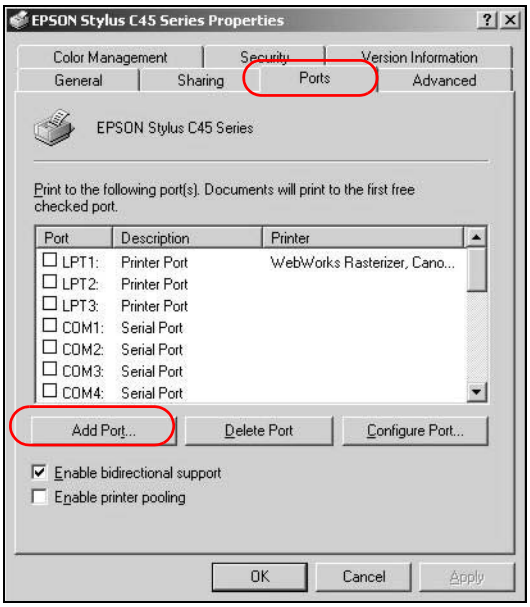
The **Printers** folder opens up. First you need to open up the properties windows for the printer you want to configure a TCP/IP port.

2 Locate your printer.

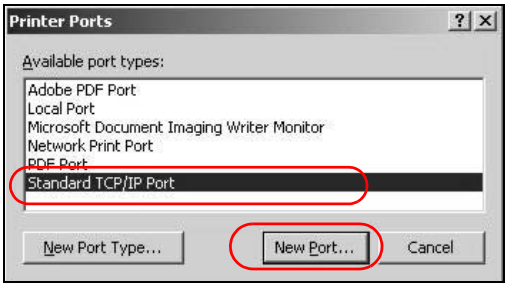
3 Right click on your printer and select **Properties**.



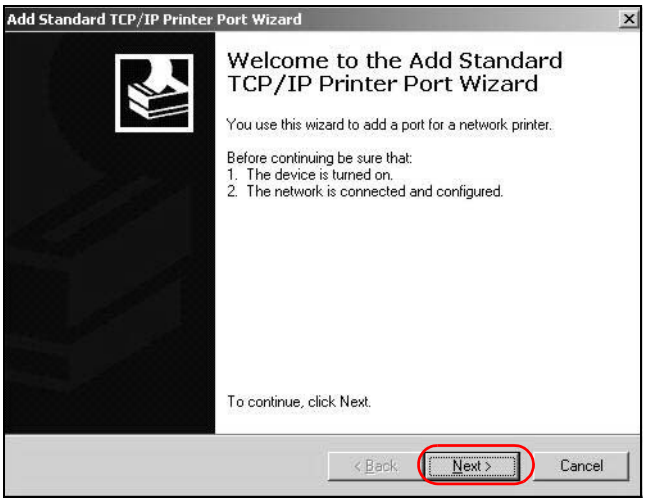
4 Select the **Ports** tab and click **Add Port...**



5 A **Printer Ports** window appears. Select **Standard TCP/IP Port** and click **New Port..**.

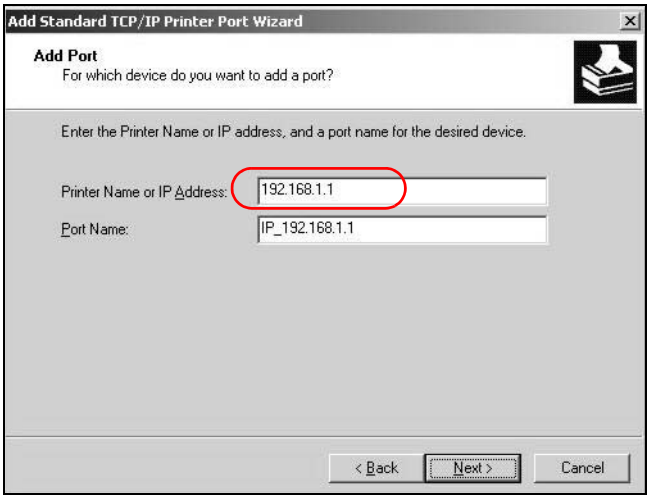


6 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

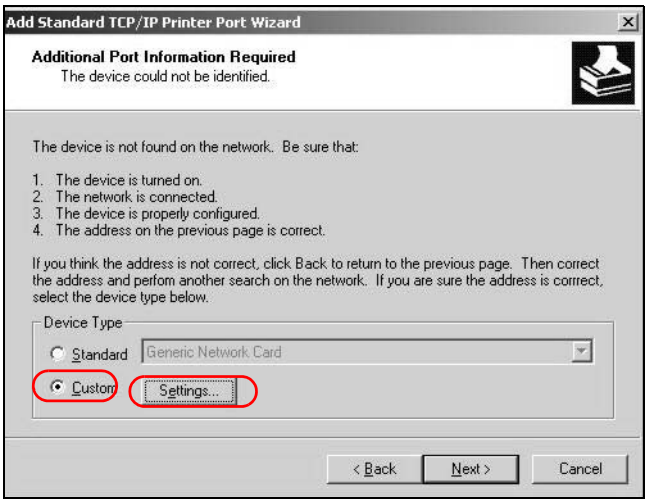

Add Standard TCP/IP Printer Port Wizard
Welcome to the Add Standard TCP/IP Printer Port Wizard
You use this wizard to add a port for a network printer.
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.
To continue, click Next.
< Back
Next >
Cancel

7 Enter the IP address of the Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
192.168.1.1
Port Name:
IP_192.168.1.1
< Back
Next >
Cancel

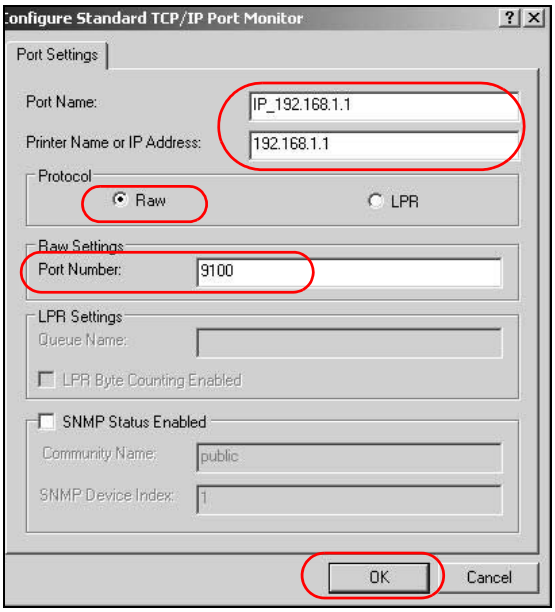
8 Select **Custom** under **Device Type** and click **Settings**.


Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perfom another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

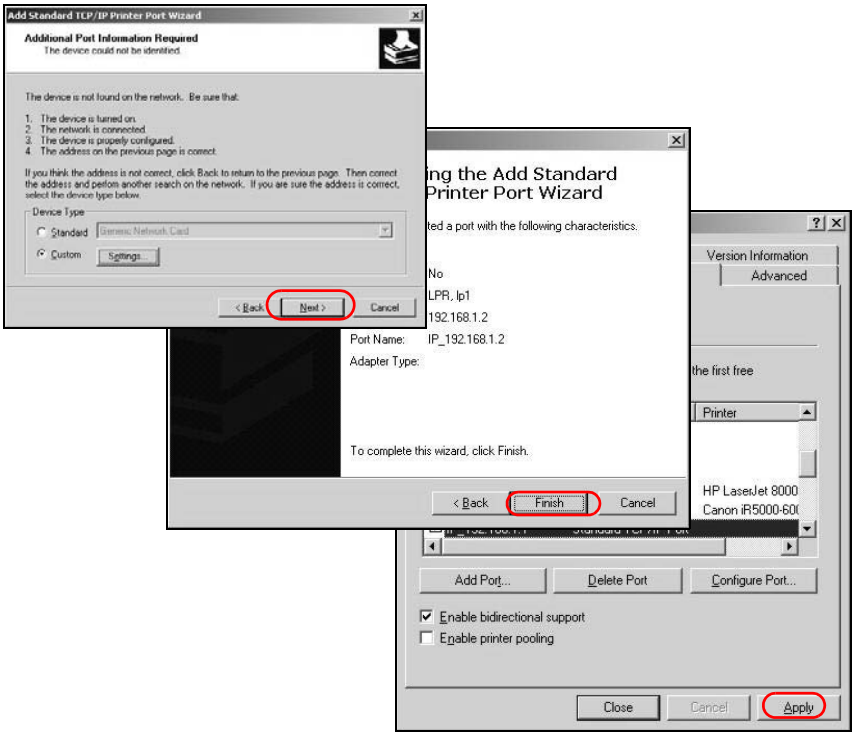
9 Confirm the IP address of the Device in the IP Address field.

10 Select **Raw** under **Protocol**.

11 The **Port Number** is automatically configured as **9100**. Click **OK**.



12 Continue through the wizard, apply your settings and close the wizard window.

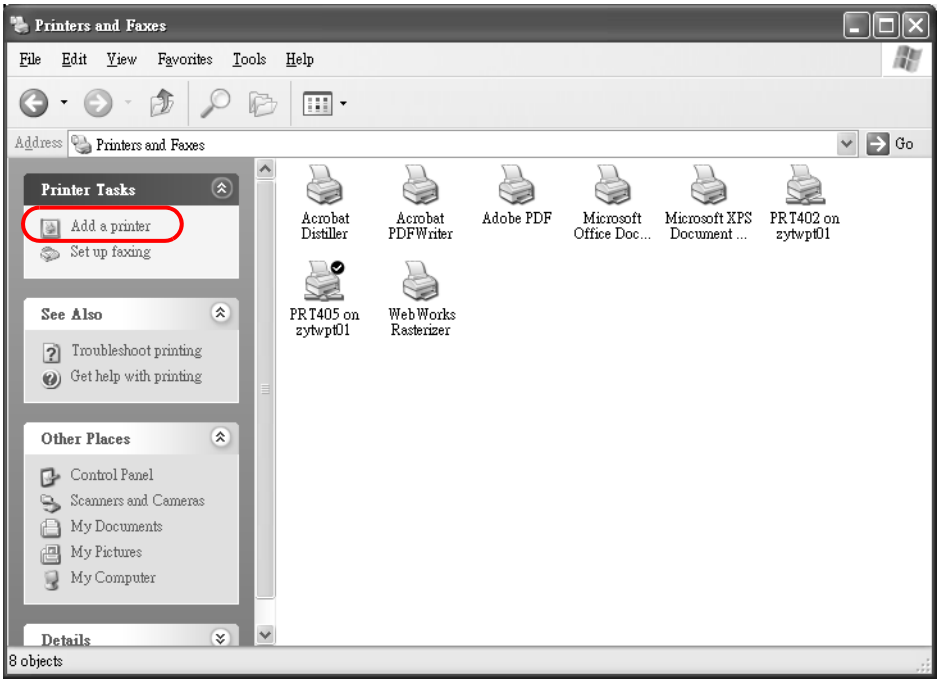

Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Custom
Settings...
< Back
Next >
Cancel
ing the Add Standard Printer Port Wizard
ted a port with the following characteristics.
No
LPR, lp1
192.168.1.2
Port Name: IP_192.168.1.2
Adapter Type:
To complete this wizard, click Finish.
< Back
Finish
Cancel
Version Information
Advanced
the first free
Printer
HP LaserJet 8000
Canon iR5000-60
Add Port...
Delete Port
Configure Port...
Enable bidirectional support
Enable printer pooling
Close
Cancel
Apply

13 Repeat steps 1 to 12 to add this printer to other computers on your network.

Add a New Printer Using Windows

This example shows how to connect a printer to your Device using the Windows XP Professional operating system. Some menu items may look different on your operating system.

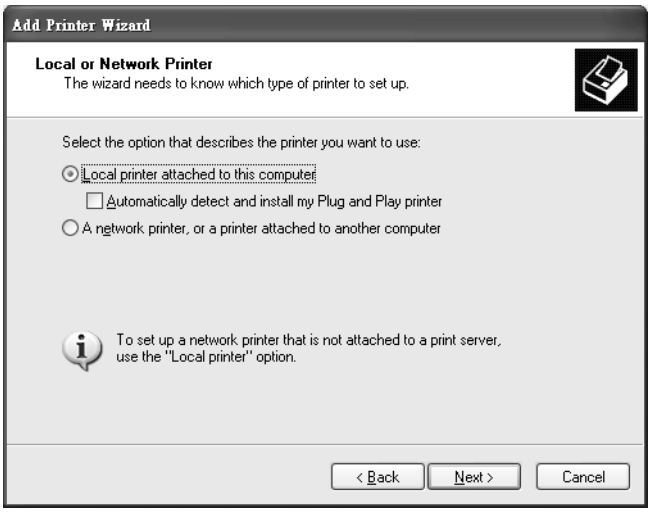
1 Click **Start** > **Control Panel** > **Printers and Faxes** to open the **Printers and Faxes** screen. Click **Add a Printer**.



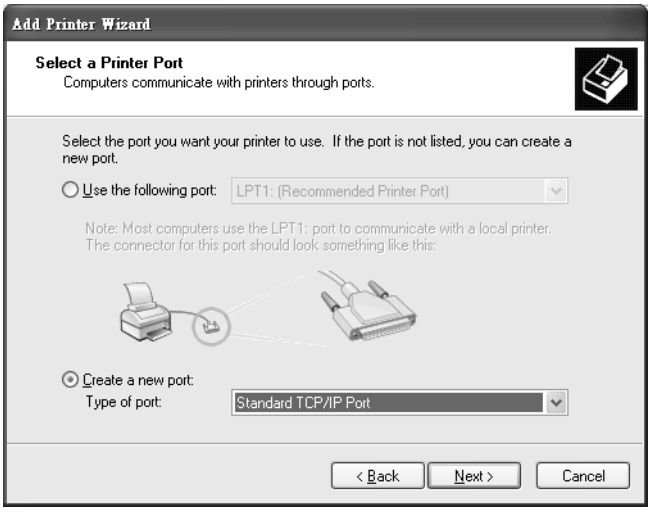
2 The **Add Printer Wizard** screen displays. Click **Next**.

Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

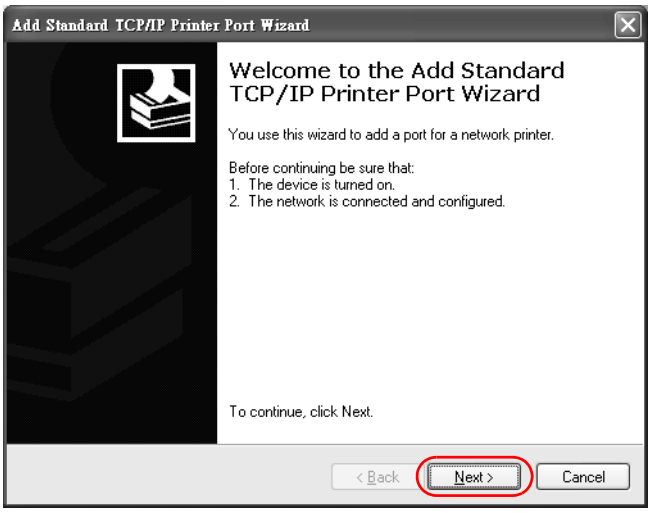
3 Select **Local printer attached to this computer** and click **Next**.


Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

4 Select **Create a new port** and **Standard TCP/IP Port**. Click **Next**.

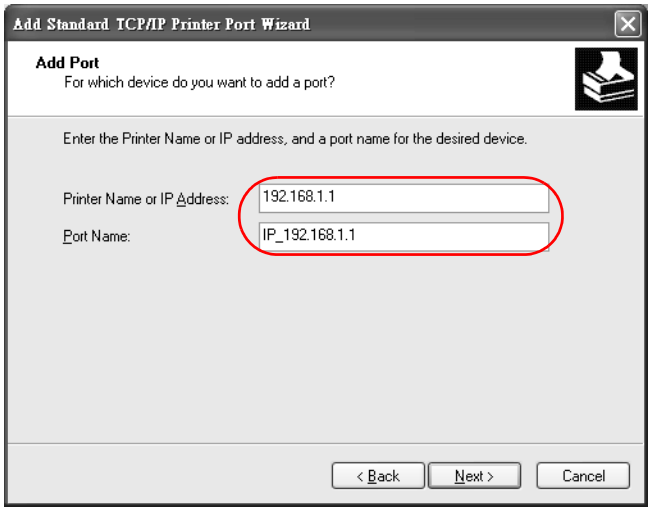

Add Printer Wizard
Select a Printer Port
Computers communicate with printers through ports.
Select the port you want your printer to use. If the port is not listed, you can create a new port.
Use the following port:
LPT1: (Recommended Printer Port)
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:
Create a new port:
Type of port:
Standard TCP/IP Port
< Back
Next >
Cancel

5 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

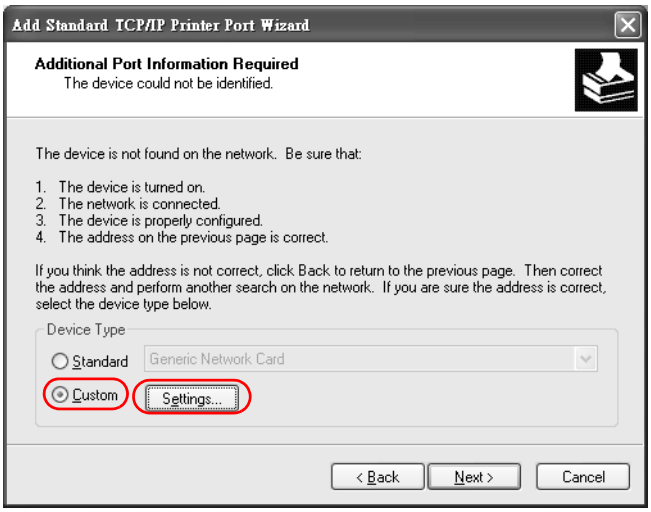

Add Standard TCP/IP Printer Port Wizard
Welcome to the Add Standard TCP/IP Printer Port Wizard
You use this wizard to add a port for a network printer.
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.
To continue, click Next.
< Back
Next >
Cancel

6 Enter the IP address of the Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
192.168.1.1
Port Name:
IP_192.168.1.1
< Back
Next >
Cancel

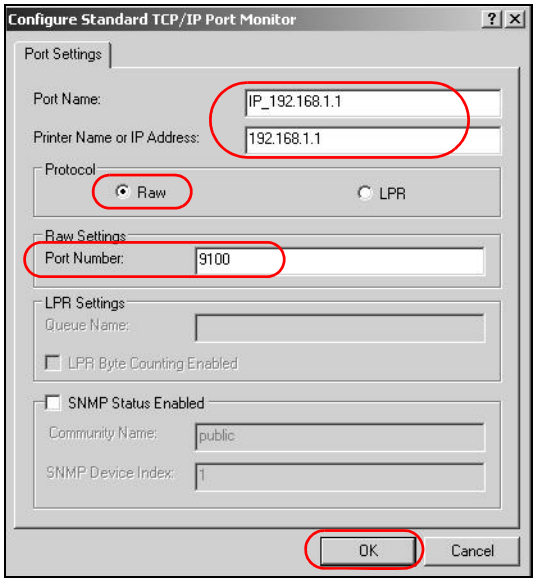
7 Select **Custom** under **Device Type** and click **Settings**.


Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

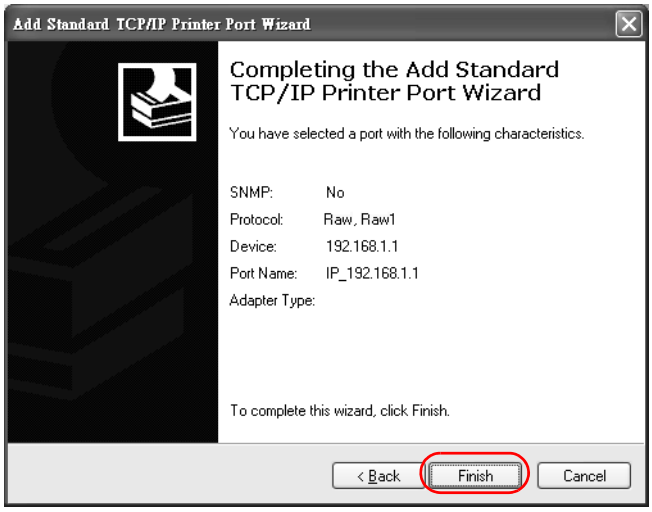
8 Confirm the IP address of the Device in the Printer **Name or IP Address** field.

9 Select **Raw** under **Protocol**.

10 The **Port Number** is automatically configured as **9100**. Click **OK** to go back to the previous screen and click **Next**.



11 Click **Finish** to close the wizard window.

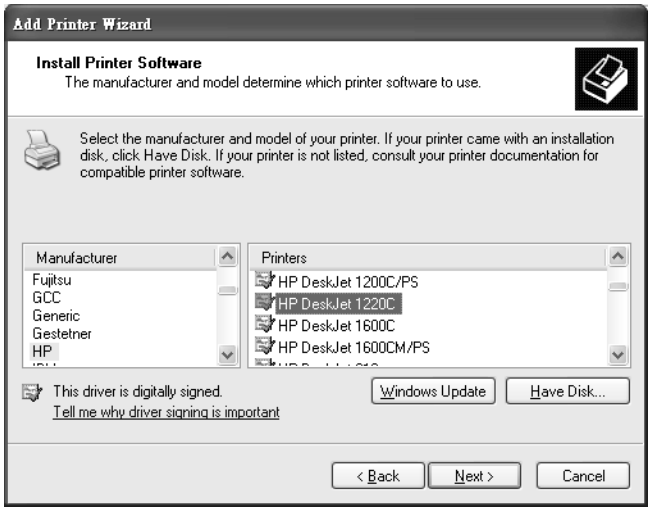


12 Select the make of the printer that you want to connect to the print server in the **Manufacturer** list of printers.

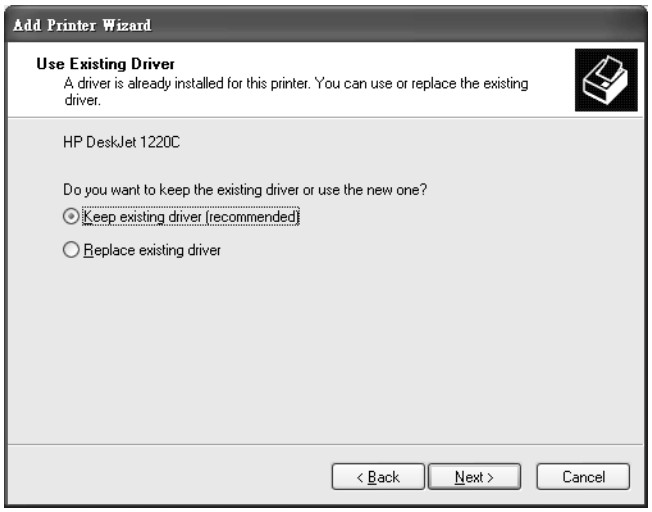
13 Select the printer model from the list of **Printers**.

14 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk...** and install the new printer driver.

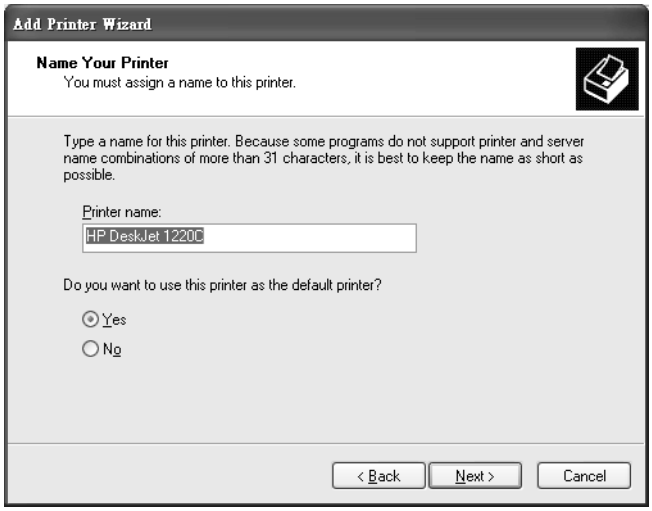
15 Click **Next** to continue.


Add Printer Wizard
Install Printer Software
The manufacturer and model determine which printer software to use.
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.
Manufacturer
Fujitsu
GCC
Generic
Gestetner
HP
Printers
HP DeskJet 1200C/PS
HP DeskJet 1220C
HP DeskJet 1600C
HP DeskJet 1600CM/PS
This driver is digitally signed.
Tell me why driver signing is important
Windows Update
Have Disk...
< Back
Next >
Cancel

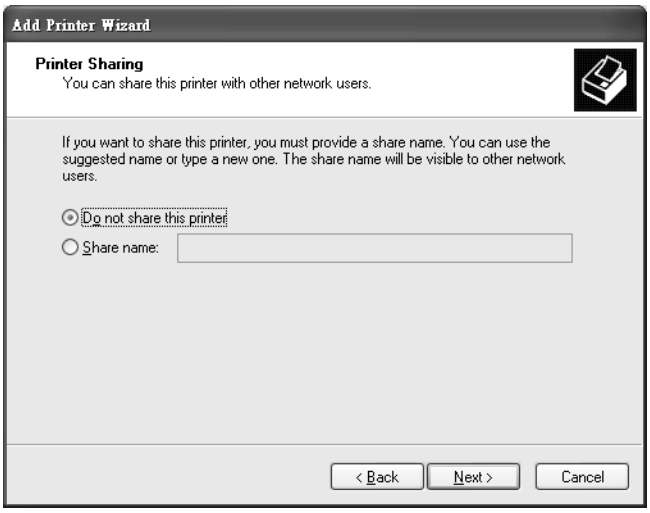
16 If the following screen displays, select **Keep existing driver** radio button and click **Next** if you already have a printer driver installed on your computer and you do not want to change it. Otherwise, select **Replace existing driver** to replace it with the new driver you selected in the previous screen and click **Next**.


Add Printer Wizard
Use Existing Driver
A driver is already installed for this printer. You can use or replace the existing driver.
HP DeskJet 1220C
Do you want to keep the existing driver or use the new one?
Keep existing driver (recommended)
Replace existing driver
< Back
Next >
Cancel

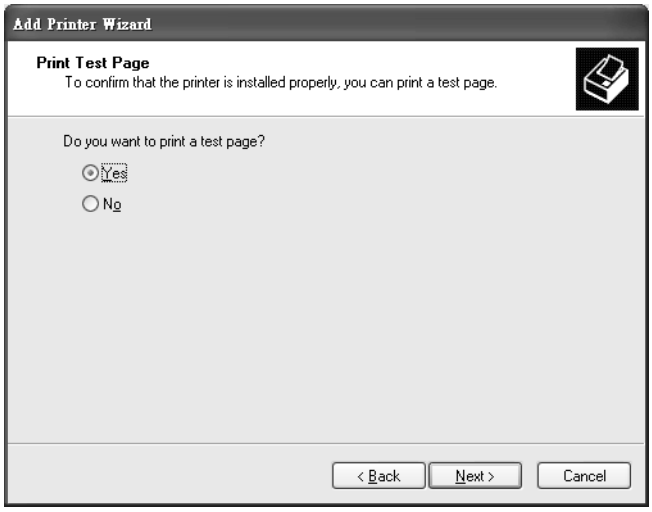
17 Type a name to identify the printer and then click **Next** to continue.


Add Printer Wizard
Name Your Printer
You must assign a name to this printer.
Type a name for this printer. Because some programs do not support printer and server name combinations of more than 31 characters, it is best to keep the name as short as possible.
Printer name:
HP DeskJet 1220C
Do you want to use this printer as the default printer?
Yes
No
< Back
Next >
Cancel

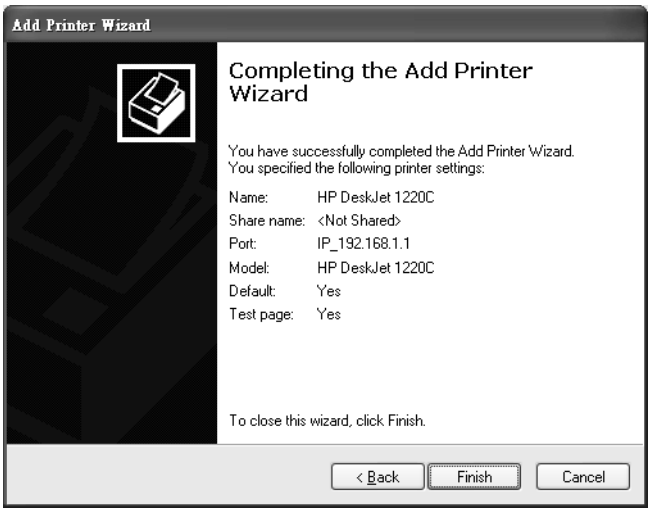
18 The Device is a print server itself and you do not need to have your computer act as a print server by sharing the printer with other users in the same network; just select **Do not share this printer** and click **Next** to proceed to the following screen.


Add Printer Wizard
Printer Sharing
You can share this printer with other network users.
If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.
Do not share this printer
Share name:
< Back
Next >
Cancel

19 Select **Yes** and then click the **Next** button if you want to print a test page. A pop-up screen displays to ask if the test page printed correctly. Otherwise select **No** and then click **Next** to continue.


Add Printer Wizard
Print Test Page
To confirm that the printer is installed properly, you can print a test page.
Do you want to print a test page?
Yes
No
< Back
Next >
Cancel

20 The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.



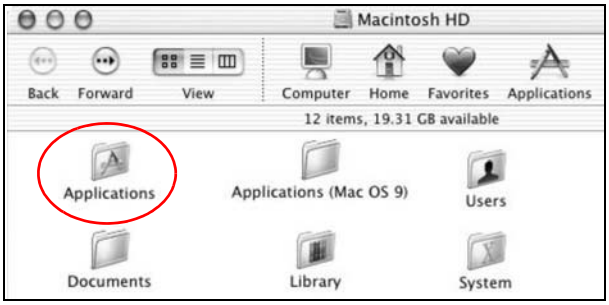
Add a New Printer Using Macintosh OS X

Complete the following steps to set up a print server driver on your Macintosh computer.

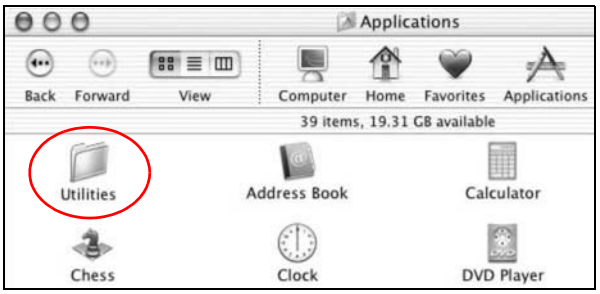
1 Click the **Print Center** icon located in the Macintosh Dock (a place holding a series of icons/ shortcuts at the bottom of the desktop). Proceed to step 6 to continue. If the **Print Center** icon is not in the Macintosh Dock, proceed to the next step.

2 On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.

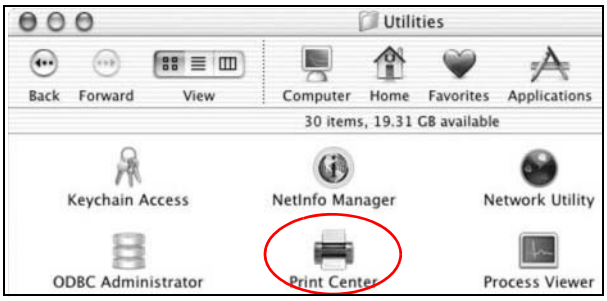
3 Double-click the **Applications** folder.



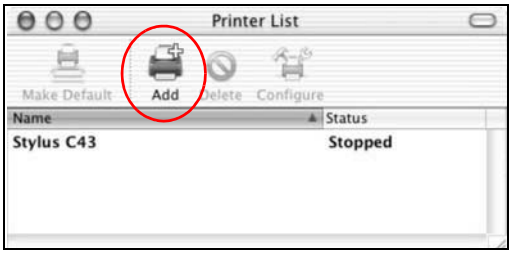
4 Double-click the **Utilities** folder.



5 Double-click the **Print Center** icon.



6 Click the **Add** icon at the top of the screen.



7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.

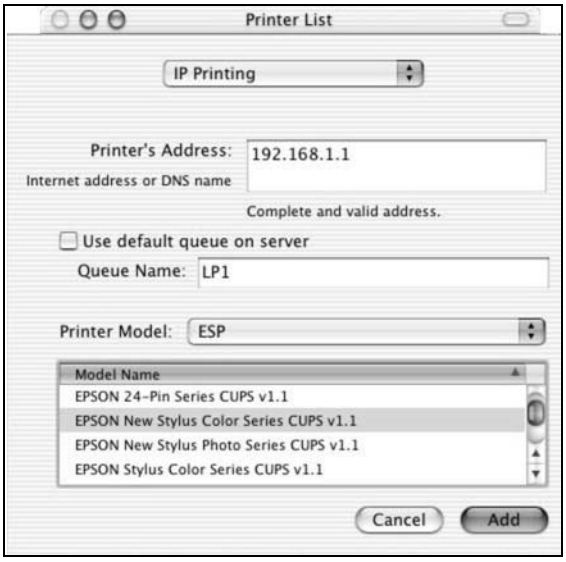
8 In the **Printer's Address** field, type the IP address of your Device.

9 Deselect the **Use default queue on server** check box.

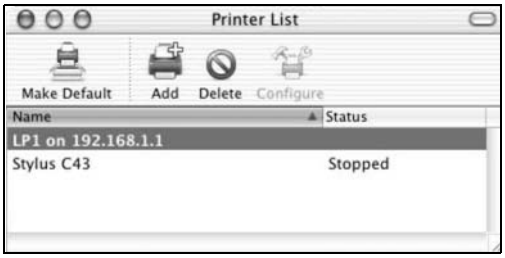
10 Type **LP1** in the **Queue Name** field.

11 Select your **Printer Model** from the drop-down list box. If the printer's model is not listed, select **Generic**.

12 Click **Add** to select a printer model, save and close the **Printer List** configuration screen.



13 The **Name LP1 on 192.168.1.1** displays in the **Printer List** field. The default printer **Name** displays in bold type.

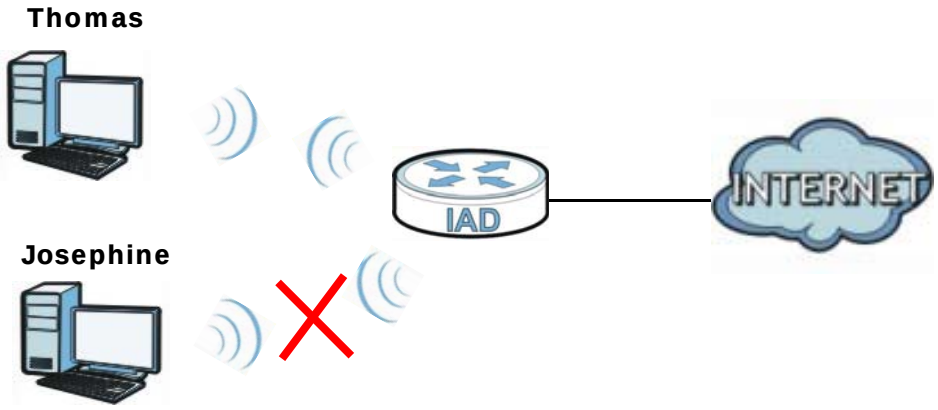


Your Macintosh print server driver setup is complete. You can now use the Device's print server to print from a Macintosh computer.

3.8 Configuring the MAC Address Filter

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



1 Click **Security** > **MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.

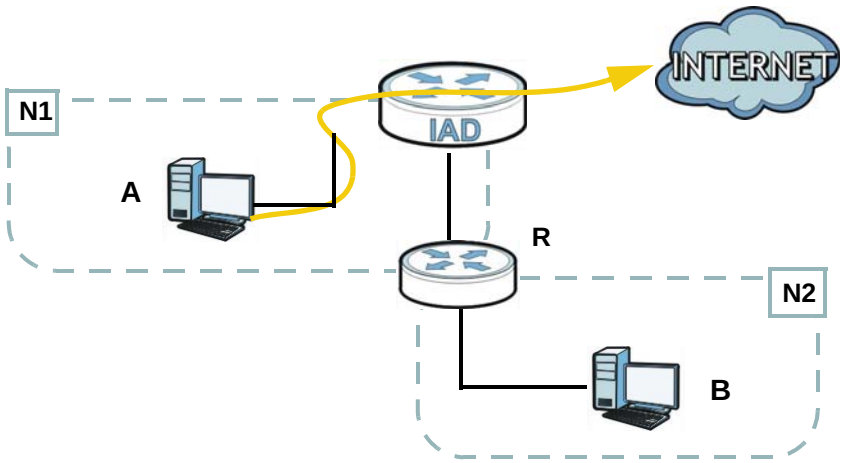
2 Find the MAC address of Thomas' computer in this screen. Select **Allow**. Click **Apply**.

Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the Device.

3.9 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.This tutorial uses the following example IP settings:

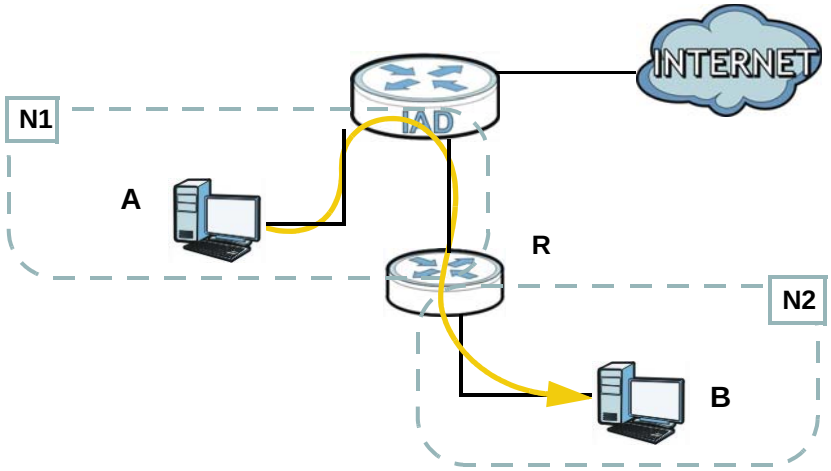
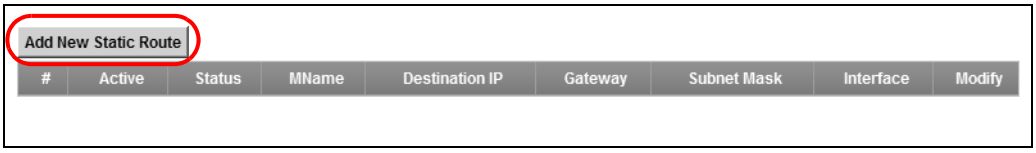


Table 3 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The Device's WAN	172.16.1.1
The Device's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

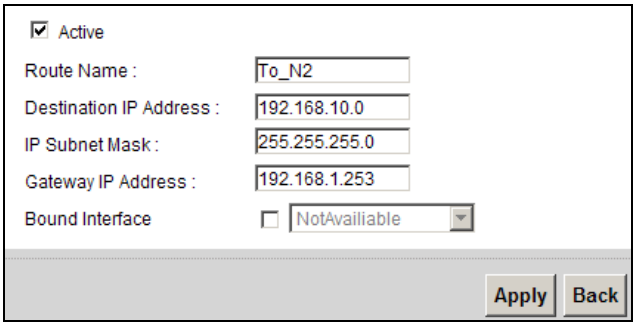
1 Click **Network Setting > Routing**. Click **Add New Static Route**.



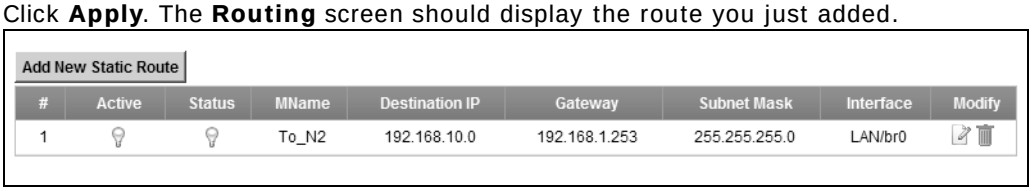
2 Configure the **Static Route Setup** screen using the following settings:

- Select **Active**.
- Specify a descriptive name for this routing rule.
- Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.

- Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.



Click **Apply**. The **Routing** screen should display the route you just added.


Add New Static Route
Active Status MName Destination IP Gateway Subnet Mask Interface Modify
1 To_N2 192.168.10.0 192.168.1.253 255.255.255.0 LAN/br0

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

3.10 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

Note: Voice traffic will not be affected by the user-defined QoS settings on the Device. It always gets the highest priority.

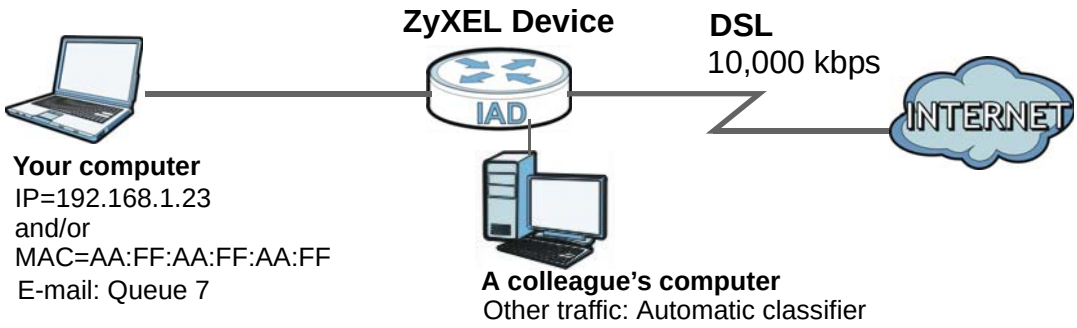
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

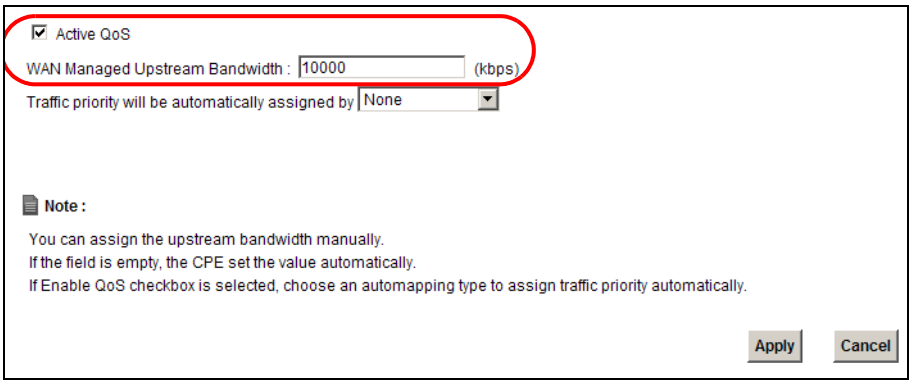
- Configure a queue to assign the highest priority queue (7) to e-mail traffic from the LAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the Device.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the Device.

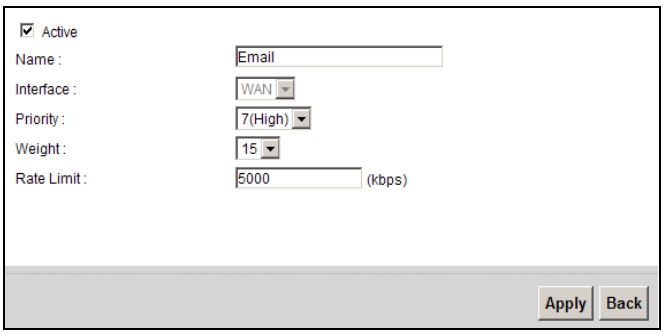


1 Click **Network Setting > QoS > General** and check **Active**. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the Device automatically determine this figure). Click **Apply** to save your settings.

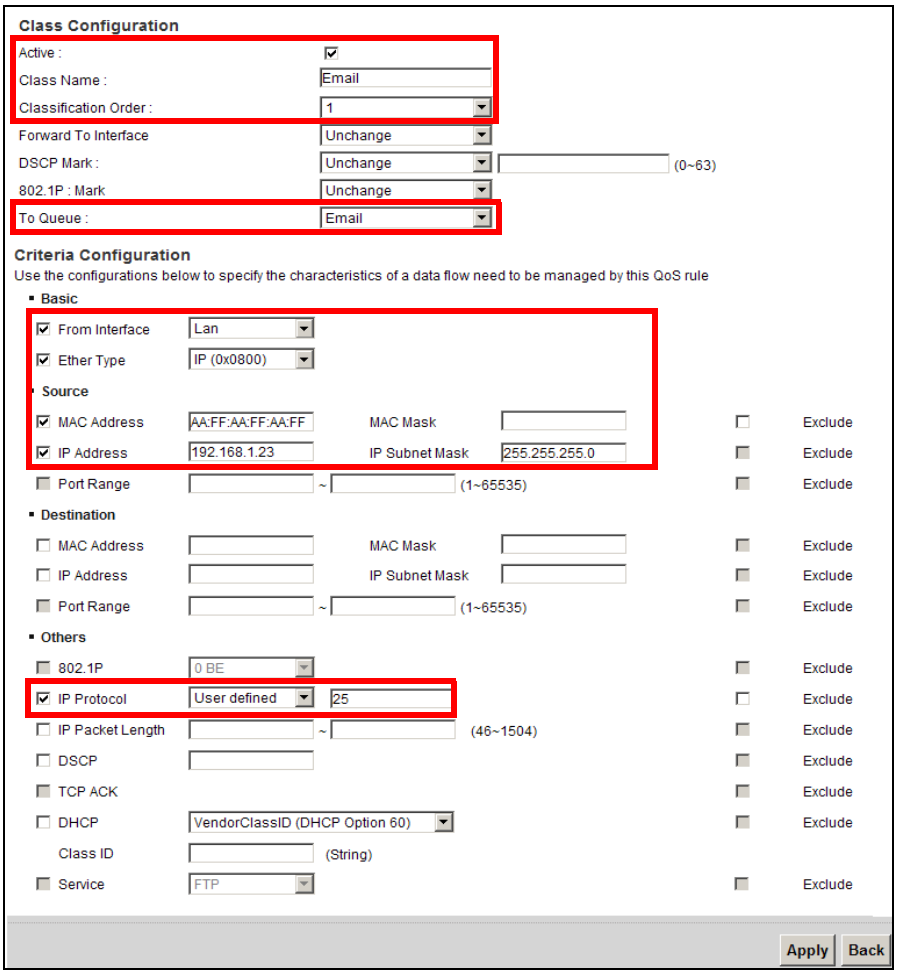

Active QoS
WAN Managed Upstream Bandwidth : 10000 (kbps)
Traffic priority will be automatically assigned by None
Note :
You can assign the upstream bandwidth manually.
If the field is empty, the CPE set the value automatically.
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.
Apply
Cancel

2 Go to **Network Setting > QoS > Queue Setup**. Click **Add new Queue** to create a new queue. In the screen that opens, check **Active** and enter or select the following values, then click **Apply**.

- **Name**: Email
- **Priority**: 7 (High)
- **Weight**: 15
- **Rate Limit**: 5,000 (kbps)



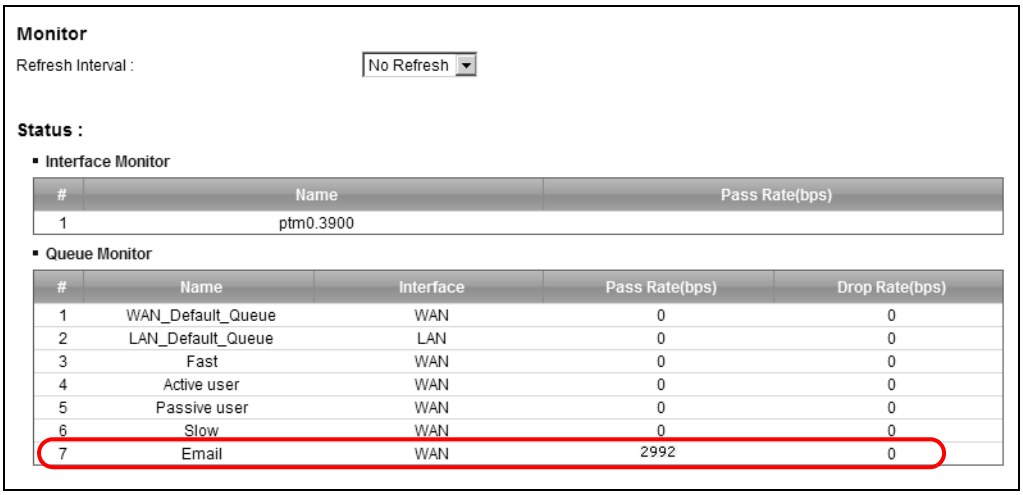
3 Go to **Network Setting > QoS > Class Setup**. Click **Add new Classifier** to create a new class. Check **Active** and follow the settings as shown in the screen below. Then click **Apply**.


Class Configuration
Active :
Class Name : Email
Classification Order : 1
Forward To Interface : Unchange
DSCP Mark : Unchange (0~63)
802.1P : Mark : Unchange
To Queue : Email
Criteria Configuration
Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule
Basic
From Interface : Lan
Ether Type : IP (0x0800)
Source
MAC Address : AA:FF:AA:FF:AA:FF MAC Mask Exclude
IP Address : 192.168.1.23 IP Subnet Mask : 255.255.255.0 Exclude
Port Range (1~65535) Exclude
Destination
MAC Address MAC Mask Exclude
IP Address IP Subnet Mask Exclude
Port Range (1~65535) Exclude
Others
802.1P : 0 BE Exclude
IP Protocol : User defined 25 Exclude
IP Packet Length (46~1504) Exclude
DSCP Exclude
TCP ACK Exclude
DHCP : VendorClassID (DHCP Option 60) Exclude
Class ID (String)
Service : FTP Exclude
Apply
Back

Class Name	Give a class name to this traffic, such as **Email** in this example.
To Queue	Link this to a queue created in the **QoS > Queue Setup** screen, which is the **Email** queue created in this example.
From Interface	This is the interface from which the traffic will be coming from. Select **Lan**.
Ether Type	Select **IP** to identify the traffic source by its IP address or MAC address.
MAC Address	Type the MAC address of your computer - **AA:FF:AA:FF:AA:FF**. Type the **MAC Mask** if you know it.
IP Address	Type the IP address of your computer - **192.168.1.23**. Type the **IP Subnet Mask** if you know it.
IP Protocol	Select **User defined** and enter **25** as the IP Protocol.

This maps e-mail traffic to queue 7 created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to queue 7 (see the **Source** fields).

4 Verify that the queue setup works by checking **Network Setting > QoS > Monitor**. This shows the bandwidth allotted to e-mail traffic compared to other network traffic.



Monitor

Refresh Interval : No Refresh

Status :

▪ Interface Monitor

#	Name	Pass Rate(bps)
1	ptm0.3900	

▪ Queue Monitor

#	Name	Interface	Pass Rate(bps)	Drop Rate(bps)
1	WAN_Default_Queue	WAN	0	0
2	LAN_Default_Queue	LAN	0	0
3	Fast	WAN	0	0
4	Active user	WAN	0	0
5	Passive user	WAN	0	0
6	Slow	WAN	0	0
7	Email	WAN	2992	0

3.11 Access the Device Using DDNS

If you connect your Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Device using a domain name.

To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial shows you how to:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your Device
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

3.11.1 Registering a DDNS Account on www.dyndns.org

1 Open a browser and type **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

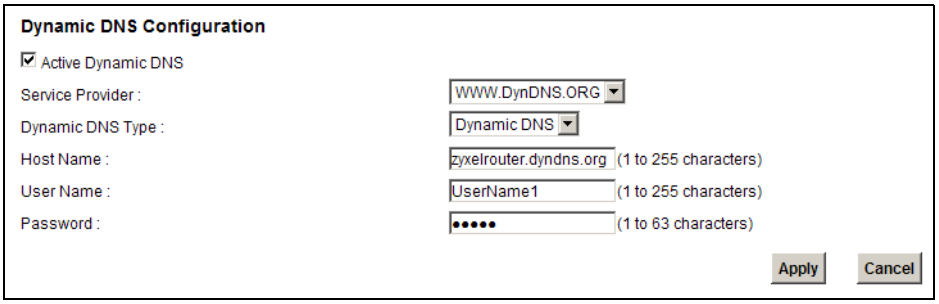
- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your Device is currently using. You can find the IP address on the Device's web configurator **Status** page.

Then you will need to configure the same account and host name on the Device later.

3.11.2 Configuring DDNS on Your Device

Configure the following settings in the **Network Setting** > **Dynamic DNS** screen.

- Select **Active Dynamic DNS**.
- Select **Dynamic DNS** for the DDNS type.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**).



Click **Apply**.

3.11.3 Testing the DDNS Setting

Now you should be able to access the Device from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

3 The Device's login page should appear. You can then log into the Device and manage it.

PART II
Technical Reference

The appendices provide general information. Some details may not apply to your Device.

4

Connection Status and System Info

4.1 Overview

After you log into the web configurator, the **Connection Status** screen appears. This shows the network connection status of the Device and clients connected to it.

Use the **System Info** screen to look at the current status of the device, system resources, interfaces (LAN, WAN and WLAN), and SIP accounts. You can also register and unregister SIP accounts.

If you click **Virtual Device** on the **System Info** screen, a visual graphic appears, showing the connection status of the Device's ports. See Section 2.2.2 on page 26 for more information.

4.2 The Connection Status Screen

Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem.

If you prefer to view the status in a list, click **List View** in the **Viewing mode** selection box. You can configure how often you want the Device to update this screen in **Refresh Interval**.

Figure 10 Connection Status: Icon View

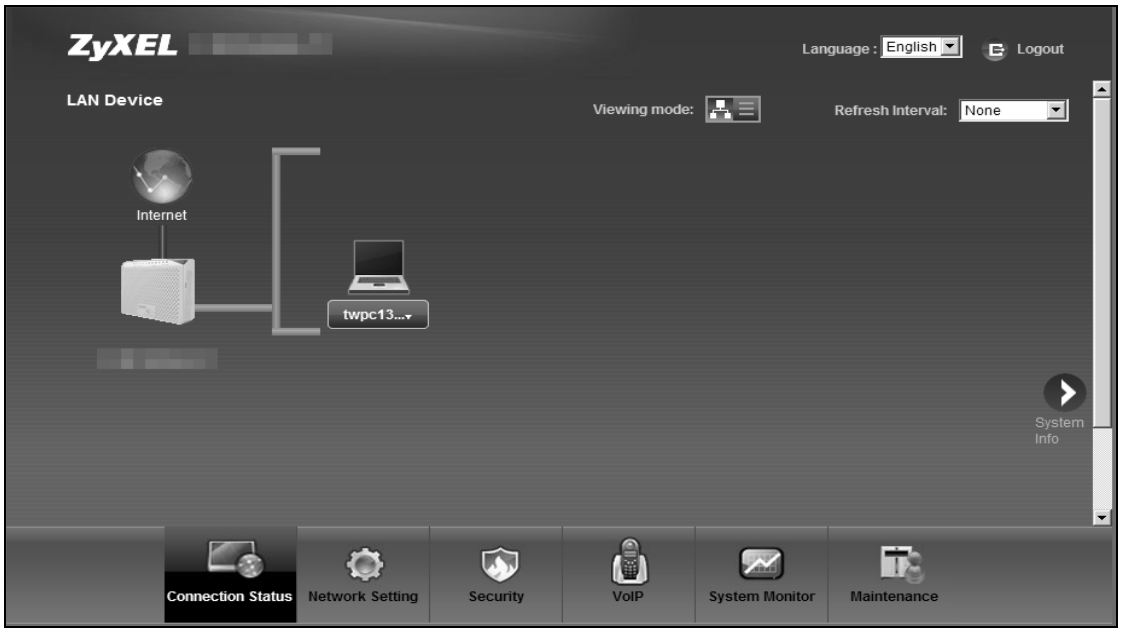
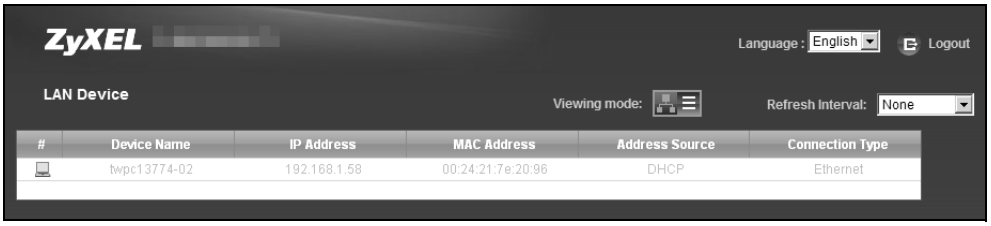


Figure 11 Connection Status: List View



In **Icon View**, if you want to view information about a client, click the client's name and **Info**. Click the IP address if you want to change it. If you want to change the name or icon of the client, click **Change name/icon**.

In **List View**, you can also view the client's information.

4.3 The System Info Screen

Click **Connection Status > System Info** to open this screen.

Figure 12 System Info Screen

Each field is described in the following table.

Table 4 System Info Screen

LABEL	DESCRIPTION
Language	Select the web configurator language from the drop-down list box.
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Device Information	
Host Name	This field displays the Device system name. It is used for identification. You can change this in the **Maintenance > System** screen's **Host Name** field.
Model Name	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Device.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Go to the **Maintenance > Firmware Upgrade** screen to change it.
WAN Information	

Table 4 System Info Screen (continued)

LABEL	DESCRIPTION
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the Device in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP Server	This field displays what DHCP services the Device is providing to the LAN. Choices are: **Server** - The Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **None** - The Device is not providing any DHCP services to the LAN.
WLAN Information	
Channel	This is the channel number used by the Device now.
WPS Status	**Configured** displays when a wireless client has connected to the Device or WPS is enabled and wireless or wireless security settings have been configured. **Unconfigured** displays if WPS is disabled or wireless security settings have not been configured.
SSID (1~4) Information	
SSID	This is the descriptive name used to identify the Device in the wireless LAN.
Status	This shows whether or not the SSID is enabled (on).
Security Mode	This displays the type of security the Device is using in the wireless LAN.
Interface Status	
Interface	This column displays each interface the Device has.
Status	This field indicates whether or not the Device is using the interface. For the EtherWAN interface, this field displays **Up** when the Device is using the interface and **Down** when the Device is not using the interface. For the LAN interfaces, this field displays **Up** when the Device is using the interface and **Down** when the Device is not using the interface. For the WLAN interface, it displays **Active** when WLAN is enabled or **InActive** when WLAN is disabled. For the 3G interface, it displays **Enabled** when 3G is enabled or **Disabled** when 3G is disabled.
Rate	For the LAN interfaces, this displays the port speed and duplex setting. For the WAN interface, this displays the port speed and duplex setting. For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or **N/A** when WLAN is disabled. For the 3G interface, it displays the maximum transmission rate when 3G is enabled or **N/A** when 3G is disabled.
System Status	
System Up Time	This field displays how long the Device has been running since it last started up. The Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it (see Section 1.7 on page 22).
Current Date/Time	This field displays the current date and time in the Device. You can change this in **Maintenance > Time Setting**.

Table 4 System Info Screen (continued)

LABEL	DESCRIPTION
System Resource	
CPU Usage	This field displays what percentage of the Device's processing ability is currently used. When this percentage is close to 100%, the Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
Memory Usage	This field displays what percentage of the Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the Device is probably becoming unstable, and you should restart the device. See Chapter 28 on page 269, or turn off the device (unplug the power) for a few seconds.
USB Status	
Type	This shows the type of device connected to the Device.
Status	This shows whether the device is currently active (**Up**). This shows **N/A** if there are no device connected to the Device or the connected device is not working.
Registration Status	
Account	This column displays each SIP account in the Device.
Action	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. If the SIP account is already registered with the SIP server, • Click **Unregister** to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. • The second field displays **Registered**. If the SIP account is not registered with the SIP server, • Click **Register** to have the Device attempt to register the SIP account with the SIP server. • The second field displays the reason the account is not registered. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Settings**. **Register Fail** - The last time the Device tried to register the SIP account with the SIP server, the attempt failed. The Device automatically tries to register the SIP account when you turn on the Device or when you activate it.
Account Status	This shows **Active** when the SIP account has been registered and ready for use or **In-Active** when the SIP account is not yet registered.
URI	This field displays the account number and service domain of the SIP account. You can change these in **VoIP > SIP > SIP Settings**.

5

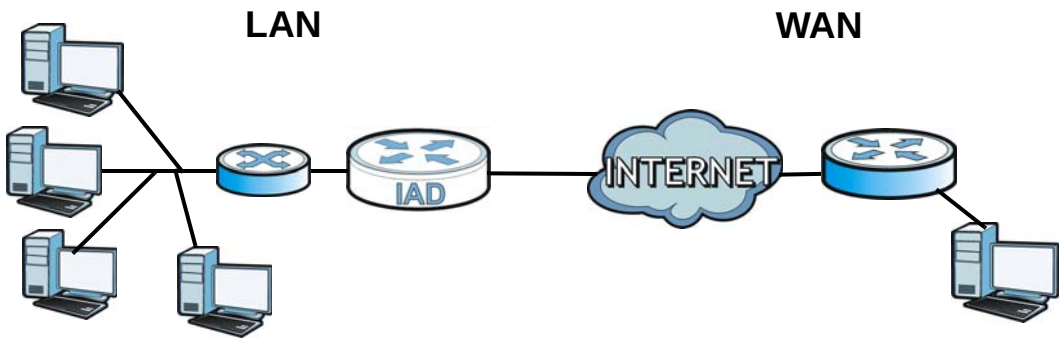
Broadband

5.1 Overview

This chapter discusses the Device's **Broadband** screens. Use these screens to configure your Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

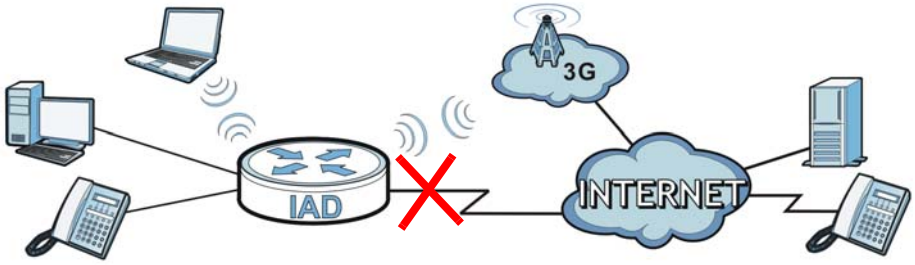
Figure 13 LAN and WAN



3G (third generation) standards for the sending and receiving of voice, video, and data in a mobile environment.

You can attach a 3G wireless adapter to the USB port and set the Device to use this 3G connection as your WAN or a backup when the wired WAN connection fails.

Figure 14 3G WAN Connection



5.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the Device for Internet access (Section 5.2 on page 84).
- Use the **3G Backup** screen to configure 3G WAN connection (Section 5.3 on page 89).

5.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the Device, which makes it accessible from an outside network. It is used by the Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

ATM

Asynchronous Transfer Mode (ATM) is a WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between Finding Out More

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses. The Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as “/x” where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

IPv6 Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block’s 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Device passes the IPv6 prefix information to LAN hosts. The hosts use the prefix to generate their IPv6 addresses.

5.1.3 Before You Begin

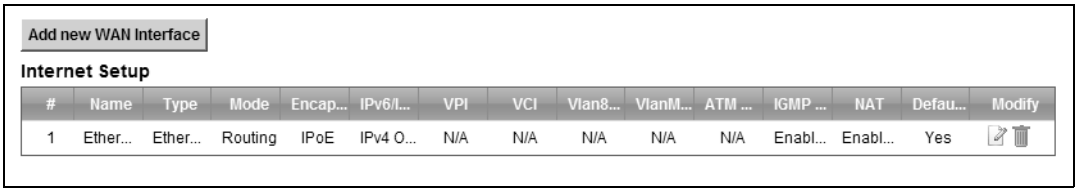
You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.2 The Broadband Screen

The Device must have a WAN interface to allow users to use the Ethernet WAN port or DSL port to access the Internet. Use the **Broadband** screen to view or modify a WAN interface.

Click **Network Setting > Broadband**. The following screen opens.

Figure 15 Network Setting > Broadband


Add new WAN Interface
Internet Setup
Name Type Mode Encap... IPv6/I... VPI VCI Vlan8... VlanM... ATM ... IGMP ... NAT Defau... Modify
1 Ether... Ether... Routing IPoE IPv4 O... N/A N/A N/A N/A N/A Enabl... Enabl... Yes

The following table describes the fields in this screen.

Table 5 Network Setting > Broadband

LABEL	DESCRIPTION
Add new WAN Interface	Click this to create a new WAN interface.
#	This is the index number of the connection.
Name	This is the service name of the connection.
Type	This shows the type of interface used by this connection.
Mode	This shows whether the connection is in routing mode or bridge mode.
Encapsulation	This shows the method of encapsulation used by this connection.
IPv6/IPv4 Mode	This shows whether the connection uses IPv6 or IPv4.
VPI	This is the Virtual Path Identifier (VPI).
VCI	This is the Virtual Channel Identifier (VCI).
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
ATM QoS	This shows the ATM Quality of Service (QoS) type configured for this connection. This displays **N/A** when there is no ATM QoS assigned.

Table 5 Network Setting > Broadband (continued)

LABEL	DESCRIPTION
IGMP Proxy	This shows whether IGMP (Internet Group Multicast Protocol) is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
NAT	This shows whether NAT is activated or not for this connection. NAT is not available when the connection uses the bridging service.
Default Gateway	This shows whether the Device uses the interface of this connection as the system default gateway.
Modify	Click the **Edit** icon to configure the connection. Click the **Delete** icon to delete this connection from the Device. A window displays asking you to confirm that you want to delete the connection.

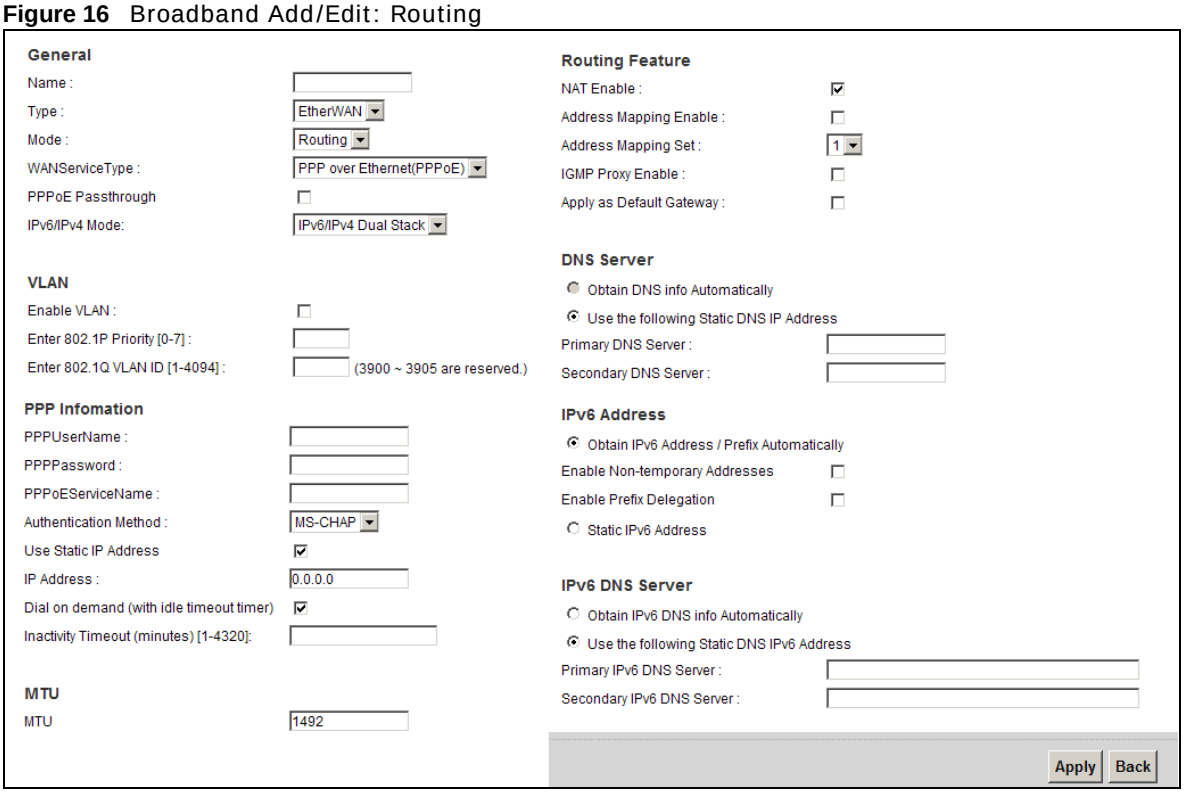
5.2.1 Add/Edit Internet Connection

Use this screen to configure a WAN connection. The screen varies depending on the interface type, encapsulation, and WAN service type you select.

5.2.1.1 Routing

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Routing** as the encapsulation mode.

Figure 16 Broadband Add/Edit: Routing



The following table describes the fields in this screen.

Table 6 Broadband Add/Edit: Routing

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	The Device transmits data over the Ethernet WAN port.
Mode	Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.
WAN Service Type	This field is available only when you select **Routing** in the **Mode** field. Select the method of encapsulation used by your ISP. • **PPP over Ethernet (PPPoE)** - PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access. • **IP over Ethernet** - In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment.
PPPoE Passthrough	This field is available when you select PPPoE encapsulation. In addition to the Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
IPv6/IPv4 Mode	If you select IPv4, the Device only runs IPv4. If you select IPv6, the Device only runs IPv6. Select **IPv6/IPv4 DualStack** to allow the Device to run IPv4 and IPv6 at the same time.
VLAN	
Enable VLAN	Select this to add the VLAN tag (specified below) to the outgoing traffic through this connection.
Enter 802.1P Priority	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
PPP Information	This section is available only when you select **Routing** in the **Mode** field and **PPPoE** in the **WAN Service Type** field.
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here.

Table 6 Broadband Add/Edit: Routing (continued)

LABEL	DESCRIPTION
Authentication Mode	The Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: • **AUTO**: Your Device accepts either CHAP or PAP when requested by this remote node. • **PAP**: Your Device accepts PAP only. • **CHAP**: Your Device accepts CHAP only. • **MS-CHAP**: Your Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
Use Static IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you want to get a dynamic IP address from the ISP.
IP Address	Enter the static IP address provided by your ISP.
Dial on demand	Select this when you don't want the connection up all the time andspecify an idle time-out in the **Inactivity Timeout field**.
Inactivity Timeout	Specify an idle time-out when you select **Dial on Demand**.
MTU	Enter the MTU (Maximum Transfer Unit) size for this traffic.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the Device act as an IGMP proxy on this connection. This allows the Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the Device use the WAN interface of this connection as the system default gateway.
DNS Server	
Obtain DNS info Automatically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
IPv6 Address	This section is not available when you select **IPv4 Only** in the **IPv6/IPv4 Mode** field.
Obtain IPv6 Address/Prefix Automatically	Select this option if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Enable Non-temporary Addresses	Select this option if you want to allow non-temporary addresses.
Enable Prefix Delegation	Select this to enable Prefix Delegation. This enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN.
Static IPv6 Address	Select this option if you have a fixed IPv6 address assigned by your ISP.

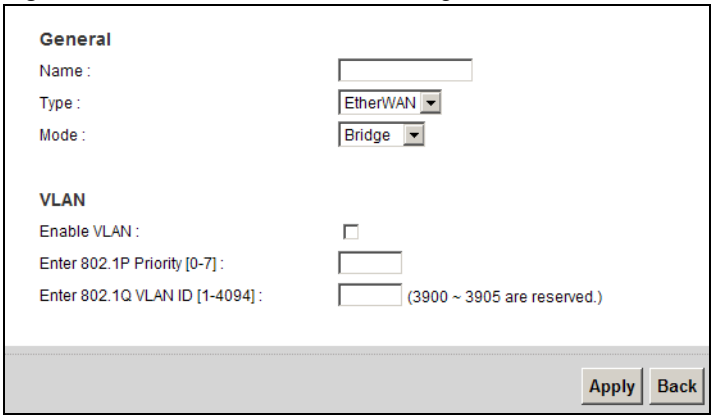
Table 6 Broadband Add/Edit: Routing (continued)

LABEL	DESCRIPTION
IPv6 Address	Enter the static IPv6 address provided by your ISP using colon (:) hexadecimal notation.
IPv6 DNS Server	Select whether you want to obtain the IPv6 DNS server addresses automatically or configure them manually.
Obtain IPv6 DNS info Automatically	Select this to have the Device get the IPv6 DNS server addresses from the ISP automatically.
Use the following Static DNS IPv6 Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary IPv6 DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

5.2.1.2 Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Bridge** as the encapsulation mode.

Figure 17 Broadband Add/Edit: Bridge



The following table describes the fields in this screen.

Table 7 Broadband Add/Edit: Bridge

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	The Device transmits data over the Ethernet WAN port.
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	

Table 7 Broadband Add/Edit: Bridge (continued)

LABEL	DESCRIPTION
Enable VLAN	Select this to add the VLAN Tag (specified below) to the outgoing traffic through this connection.
Enter 802.1P Priority	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

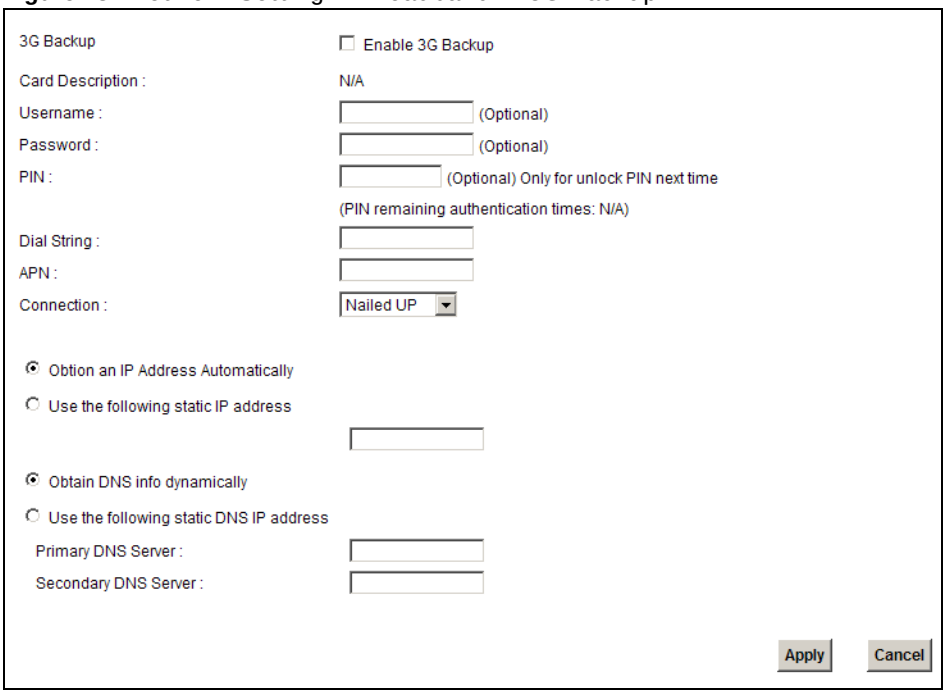
5.3 The 3G Backup Screen

Use this screen to configure your 3G settings. Click **Broadband > 3G Backup**.

Note: The actual data rate you obtain varies depending the 3G card you use, the signal strength to the service provider's base station, and so on.

If the signal strength of a 3G network is too low, the 3G card may switch to an available 2.5G or 2.75G network. Refer to Section 5.4 on page 91 for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

Figure 18 Network Setting > Broadband > 3G Backup



The following table describes the labels in this screen.

Table 8 Network Setting > Broadband > 3G Backup

LABEL	DESCRIPTION
3G Backup	Select **Enable 3G Backup** to have the Device use the 3G connection as your WAN or a backup when the wired WAN connection fails.
Card Description	This field displays the manufacturer and model name of your 3G card if you inserted one in the Device. Otherwise, it displays **N/A**.
Username	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 64 ASCII printable characters) associated with the user name above.
PIN	A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card. If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, leave this field blank.
Dial String	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number. For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan.
APN Code	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 32 ASCII printable characters. Spaces are allowed.
Connection	Select **Nailed-UP** if you do not want the connection to time out. Select **On-Demand** if you do not want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	This value specifies the time in minutes that elapses before the Device automatically disconnects from the ISP.
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use the following static IP address**.
Obtain DNS info dynamically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following static DNS IP address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to return to the previous configuration.

5.4 Technical Reference

The following section contains additional technical information about the Device features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The Device can work in bridge mode or routing mode. When the Device is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the Device queries all directly connected networks to gather group membership. After that, the Device periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Device can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

3G Comparison Table

See the following table for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

Table 9 2G, 2.5G, 2.75G, 3G and 3.5G Wireless Technologies

NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	Slow
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio. CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.		
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU[A] specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		Fast

A. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.

6

Wireless

6.1 Overview

This chapter describes the Device's **Network Setting > Wireless** screens. Use these screens to set up your Device's wireless connection.

6.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 6.2 on page 97).
- Use the **More AP** screen to set up multiple wireless networks on your Device (Section 6.3 on page 103).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 6.4 on page 105).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 6.5 on page 107).
- Use the **Scheduling** screen to schedule a time period for the wireless LAN to operate each day (Section 6.6 on page 108).
- Use the **Channel Status** screen to scan wireless LAN channel noises and view the results (Section 6.7 on page 109).

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** screen.

6.1.2 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

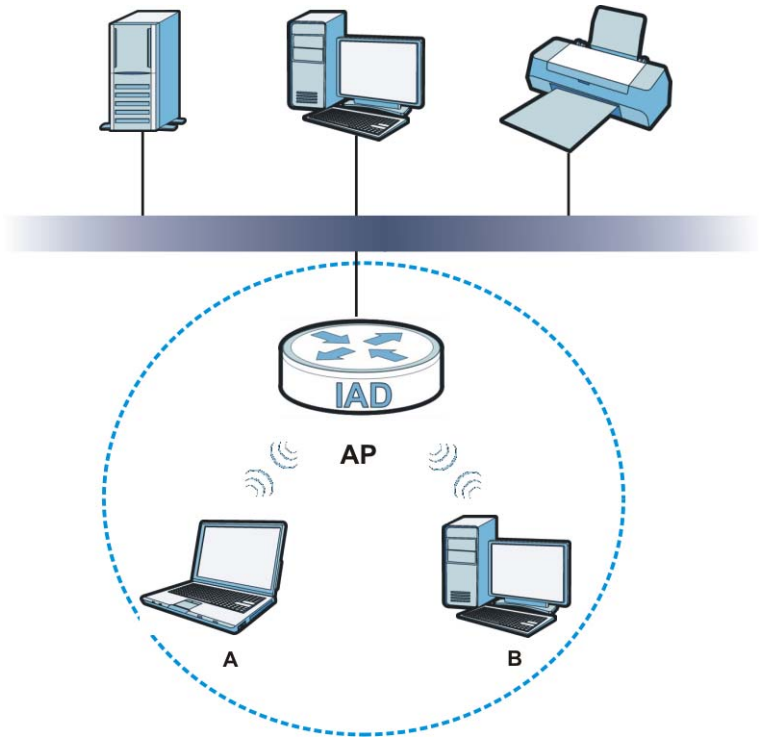
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 19 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
- Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

6.1.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 6.8 on page 109 if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

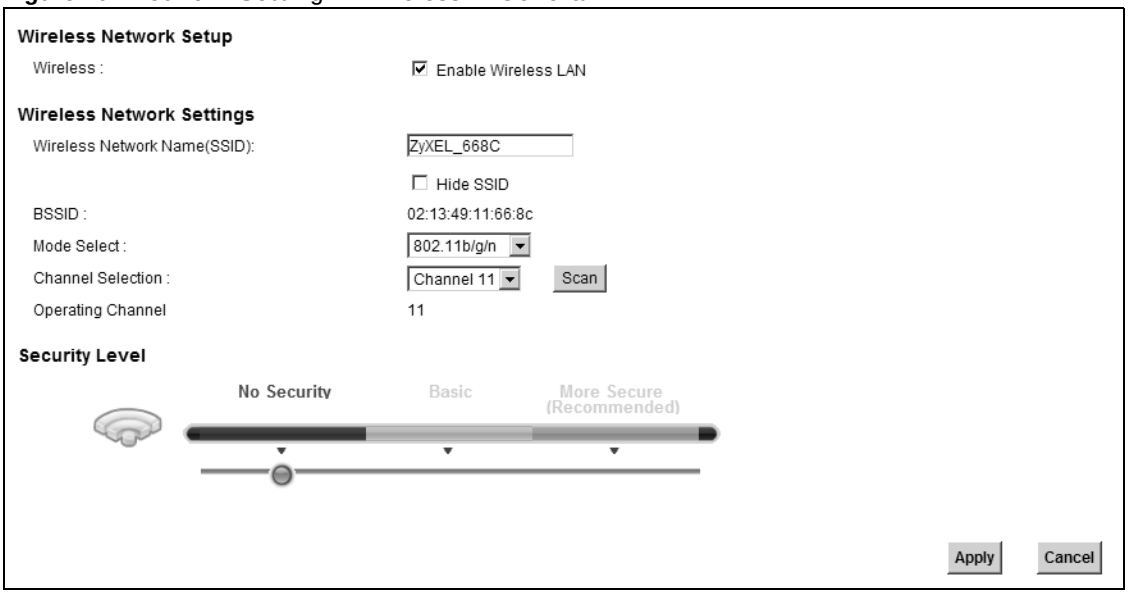
6.2 The Wireless General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the Device from a computer connected to the wireless LAN and you change the Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Device's new settings.

Click **Network Setting > Wireless** to open the **General** screen. Select the **Enable Wireless LAN** checkbox to show the Wireless configurations.

Figure 20 Network Setting > Wireless > General



The following table describes the labels in this screen.

Table 10 Network > Wireless LAN > General

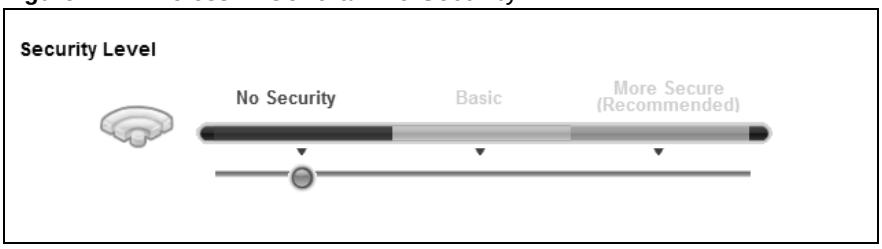
LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select the **Enable Wireless LAN** check box to activate the wireless LAN.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled.
Mode Select	This makes sure that only compliant WLAN devices can associate with the Device. Select **802.11b/g/n** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Device. The transmission rate of your Device might be reduced. Select **802.11b/g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the Device. The transmission rate of your Device might be reduced. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Device.
Channel Selection	Set the channel depending on your particular region. Select a channel or use **Auto** to have the Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the Device is currently using then displays in the **Operating Channel** field.
Scan	Click this button to have the Device immediately scan for and select a channel (which is not used by another device) whenever the device reboots or the wireless setting is changed.
Operating Channel	This is the channel currently being used by your AP.
Security Level	
Security Mode	Select **Basic** or **More Secure** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about wireless security modes.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to restore your previously saved settings.

6.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your Device, your network is accessible to any wireless networking device that is within range.

Figure 21 Wireless > General: No Security



The following table describes the labels in this screen.

Table 11 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose **No Security** from the sliding bar.

6.2.2 Basic (Static WEP/Shared WEP Encryption)

WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

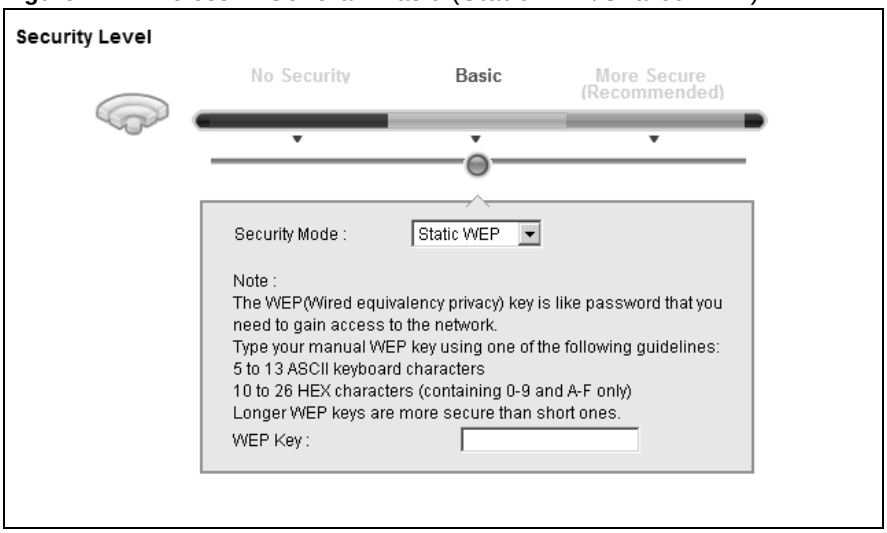
There are two types of WEP authentication namely, Open System (**Static WEP**) and Shared Key (**Shared WEP**).

Open system is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.

Shared key mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.

In order to configure and enable WEP encryption, click **Network Settings > Wireless** to display the **General** screen. Select **Basic** as the security level. Then select **Static WEP** or **Shared WEP** from the **Security Mode** list.

Figure 22 Wireless > General: Basic (Static WEP/Shared WEP)


Security Level
No Security
Basic
More Secure
(Recommended)
Security Mode :
Static WEP
Note :
The WEP(Wired equivalency privacy) key is like password that you need to gain access to the network.
Type your manual WEP key using one of the following guidelines:
5 to 13 ASCII keyboard characters
10 to 26 HEX characters (containing 0-9 and A-F only)
Longer WEP keys are more secure than short ones.
WEP Key :

The following table describes the labels in this screen.

Table 12 Wireless > General: Basic (Static WEP/Shared WEP)

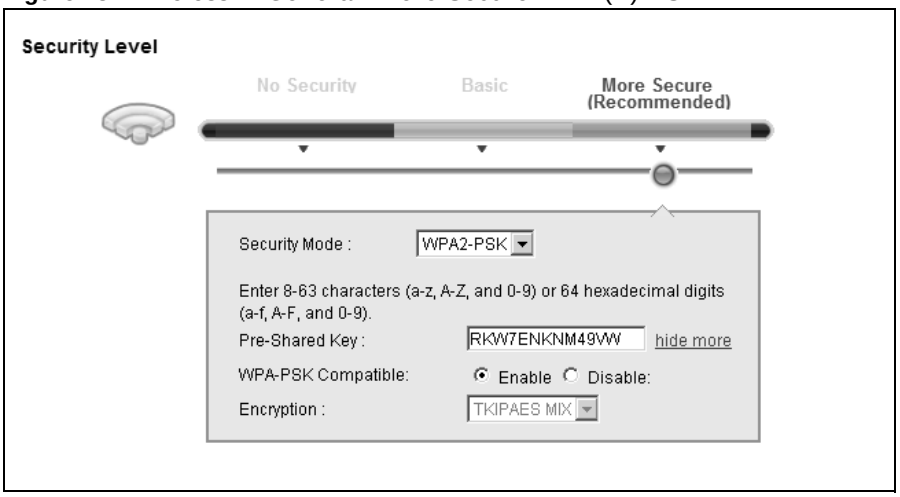
LABEL	DESCRIPTION
Security Mode	Choose **Static WEP** or **Shared WEP** from the drop-down list box. • Select **Static WEP** to have the Device allow association with wireless clients that use Open System mode. Data transfer is encrypted as long as the wireless client has the correct WEP key for encryption. The Device authenticates wireless clients using Shared Key mode that have the correct WEP key. • Select **Shared WEP** to have the Device authenticate only those wireless clients that use Shared Key mode and have the correct WEP key.
WEP Key	Enter a WEP key that will be used to encrypt data. Both the Device and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5 or 13 characters (ASCII string) or 10 or 26 hexadecimal characters ("0-9", "A-F") for a 64-bit or 128-bit WEP key respectively.

6.2.3 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Click **Network Settings** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 23 Wireless > General: More Secure: WPA(2)-PSK



The following table describes the labels in this screen.

Table 13 Wireless > General: WPA(2)-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Pre-Shared Key	The encryption mechanisms used for **WPA / WPA2** and **WPA-PSK / WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK / WPA2-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters or 64 hexidecimal digits.
more.../hide more	Click **more...** to show more fields in this section. Click **hide more** to hide them.

Table 13 Wireless > General: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
WPA-PSK Compatible	This field appears when you choose **WPA-PSK2** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your Device. The Device supports WPA-PSK and WPA2-PSK simultaneously.
Encryption	If the security mode is **WPA-PSK**, the encryption mode is set to **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. If the security mode is **WPA-PSK2** and **WPA-PSK Compatible** is disabled, the encryption mode is set to **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. If the security mode is **WPA-PSK2** and **WPA-PSK Compatible** is enabled, the encryption mode is set to **TKIPAES MIX** to allow both TKIP and AES types of security in your wireless network.

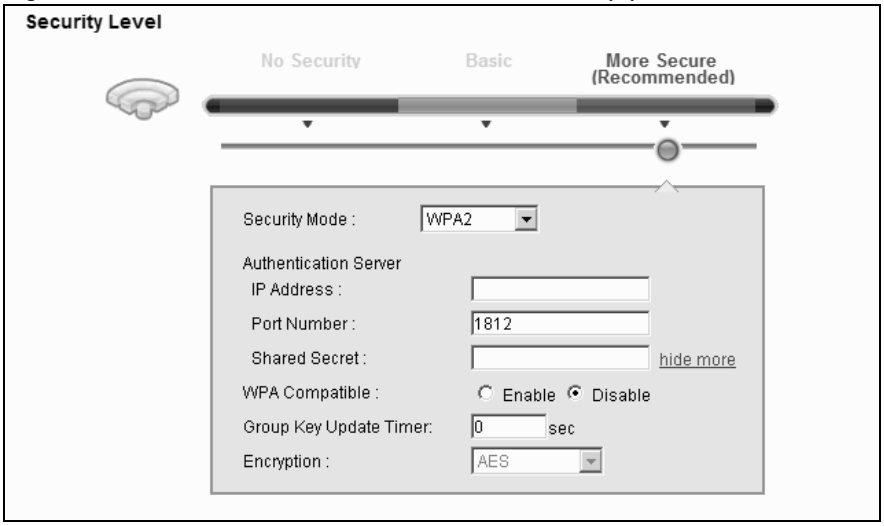
6.2.4 WPA(2) Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

Click **Network Settings** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA** or **WPA2** from the **Security Mode** list.

Figure 24 Wireless > General: More Secure: WPA(2)



The following table describes the labels in this screen.

Table 14 Wireless > General: More Secure: WPA(2)

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the Device. The key must be the same on the external authentication server and your Device. The key is not sent over the network.
more.../hide more	Click **more...** to show more fields in this section. Click **hide more** to hide them.
WPA Compatible	This field is only available for WPA2. Select this if you want the Device to support WPA and WPA2 simultaneously.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients. If the value is set to "0", the update timer function is disabled.
Encryption	If the security mode is **WPA**, the encryption mode is set to **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. If the security mode is **WPA2**, the encryption mode is set to **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP.

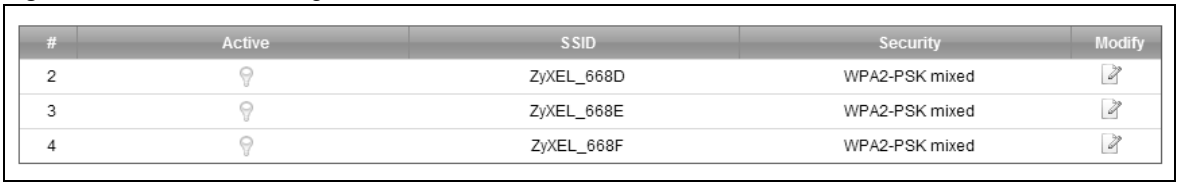
6.3 The More AP Screen

The Device can broadcast up to four wireless network names at the same time. This means that users can connect to the Device using different SSIDs. You can secure the connection on each SSID profile so that wireless clients connecting to the Device using different SSIDs cannot communicate with each other.

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the Device.

Click **Network Settings > Wireless** > **More AP**. The following screen displays.

Figure 25 Network Settings > Wireless > More AP



The following table describes the labels in this screen.

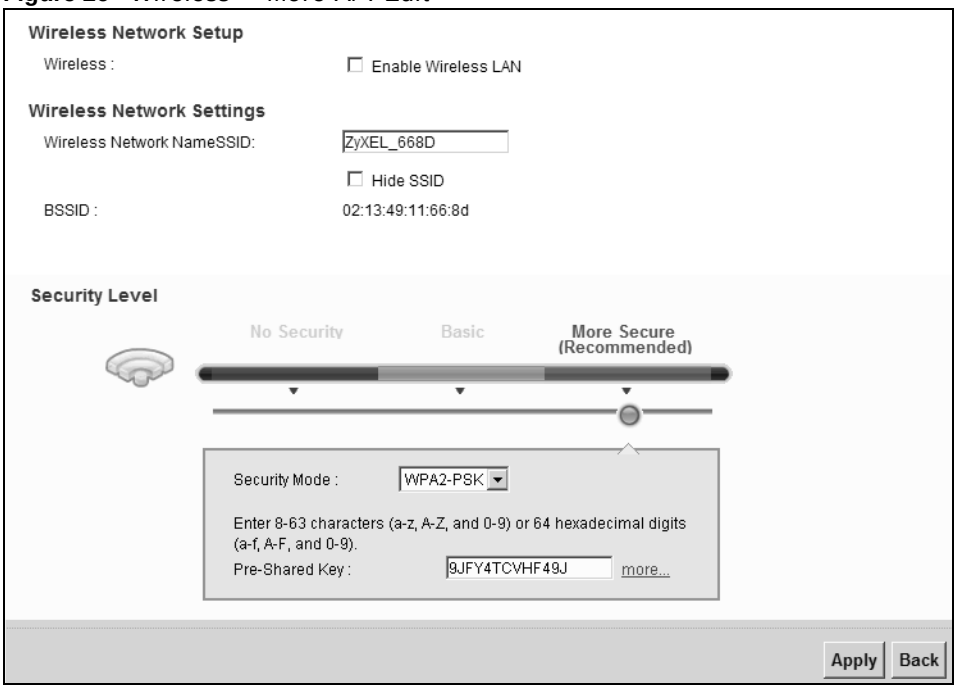
Table 15 Network Settings > Wireless > More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Active	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the **Edit** icon to configure the SSID profile.

6.3.1 Edit More AP

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 26 Wireless > More AP: Edit



The following table describes the fields in this screen.

Table 16 Wireless > More AP: Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select the **Enable Wireless LAN** check box to activate the wireless LAN.
Wireless Network Settings	

Table 16 Wireless > More AP: Edit (continued)

LABEL	DESCRIPTION
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled.
Security Level	
Security Mode	Select **Basic (WEP)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 6.2.1 on page 98 for more details about this field.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

6.4 The WPS Screen

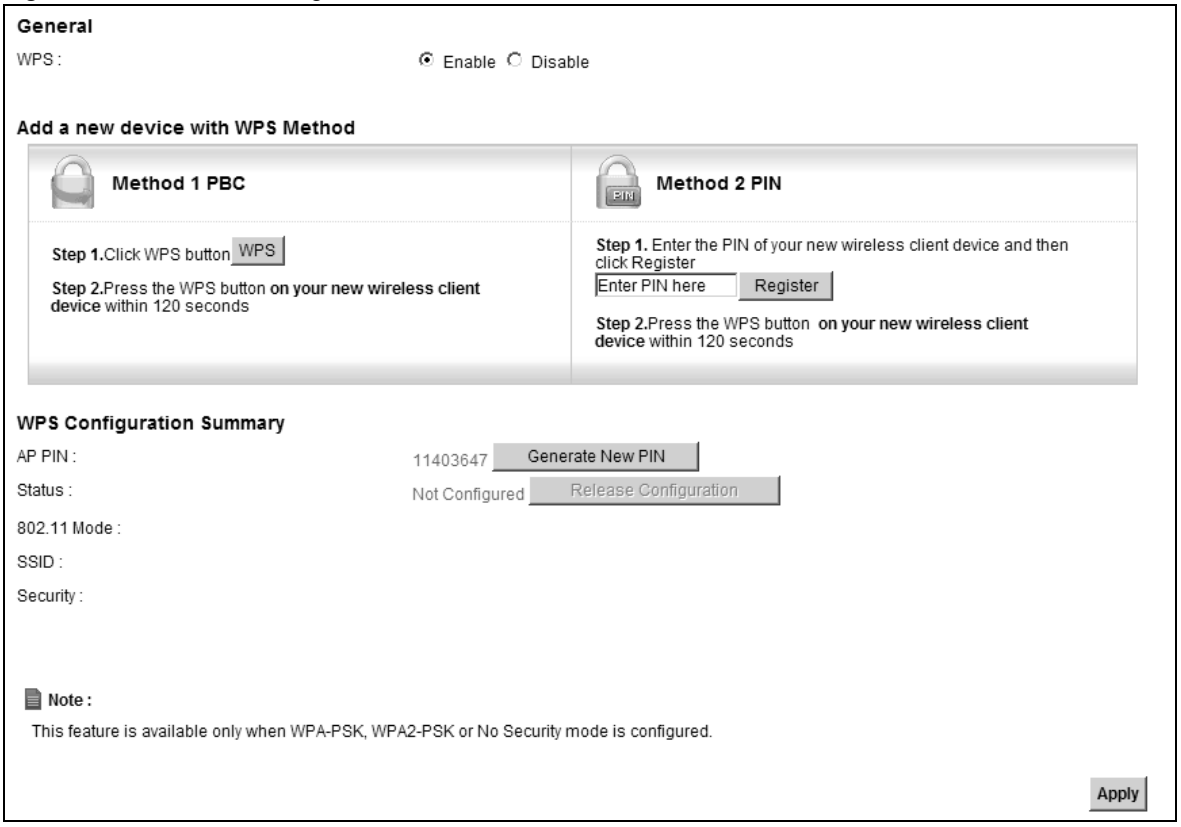
Use this screen to configure WiFi Protected Setup (WPS) on your Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See Section 6.8.5.3 on page 116 for more information about WPS.

Note: The Device applies the security settings of the **SSID1** profile (see Section 6.2 on page 97). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA-PSK**, **WPA2-PSK** or **No Security**.

Click **Network Setting > Wireless > WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 27 Network Setting > Wireless > WPS


General
WPS :
Enable
Disable
Add a new device with WPS Method
Method 1 PBC
Step 1.Click WPS button
WPS
Step 2.Press the WPS button on your new wireless client device within 120 seconds
Method 2 PIN
Step 1. Enter the PIN of your new wireless client device and then click Register
Enter PIN here
Register
Step 2.Press the WPS button on your new wireless client device within 120 seconds
WPS Configuration Summary
AP PIN :
11403647
Generate New PIN
Status :
Not Configured
Release Configuration
802.11 Mode :
SSID :
Security :
Note :
This feature is available only when WPA-PSK, WPA2-PSK or No Security mode is configured.
Apply

The following table describes the labels in this screen.

Table 17 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
Enable WPS	Select **Enable** to activate WPS on the Device.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
WPS	Click this button to add another WPS-enabled wireless device (within wireless range of the Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **WPS** button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2 PIN	Use this section to set up a WPS wireless network by entering the PIN (Personal Identification Number) of the client into the Device.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Device.
WPS Configuration Summary	

Table 17 Network Setting > Wireless > WPS (continued)

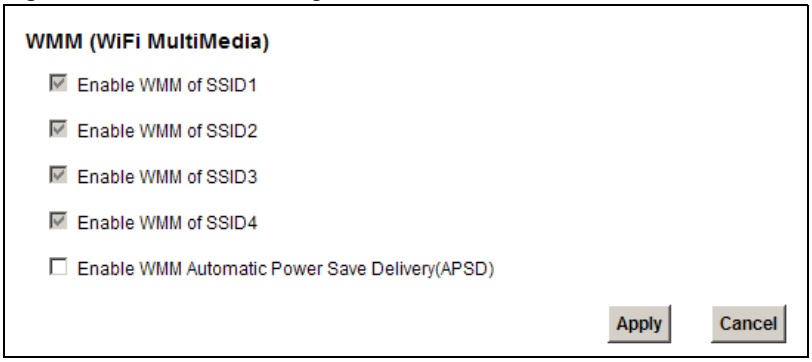
LABEL	DESCRIPTION
AP PIN	The PIN of the Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the **Generate New PIN** button to have the Device create a new PIN.
Status	This displays **Configured** when the Device has connected to a wireless network using WPS or **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Not Configured** when there is no wireless or wireless security changes on the Device or you click **Release Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is available when the WPS status is **Configured.** Click this button to remove all configured wireless and wireless security settings for WPS connections on the Device.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the Device.
SSID	This is the name of the wireless network.
Security	This is the type of wireless security employed by the network.
Apply	Click **Apply** to save your changes.

6.5 The WMM Screen

Use this screen to enable or disable Wi-Fi MultiMedia (WMM) wireless networks for multimedia applications.

Click **Network Setting > Wireless > WMM**. The following screen displays.

Figure 28 Network Setting > Wireless > WMM



The following table describes the labels in this screen.

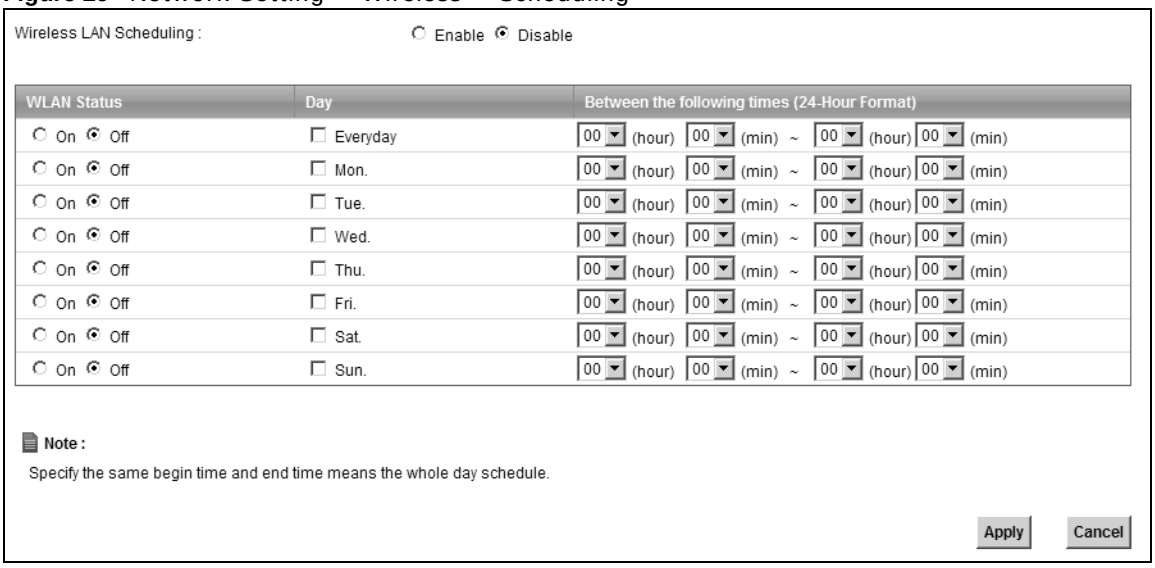
Table 18 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
Enable WMM of SSID1~4	This enables the Device to automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Enable WMM Automatic Power Save Deliver (APSD)	Click this to increase battery life for battery-powered wireless clients. APSD uses a longer beacon interval when transmitting traffic that does not require a short packet exchange interval.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.6 Scheduling Screen

Click **Network Setting > Wireless > Scheduling** to open the **Wireless LAN Scheduling** screen. Use this screen to configure when the Device enables or disables the wireless LAN.

Figure 29 Network Setting > Wireless > Scheduling



The following table describes the labels in this screen.

Table 19 Network Setting > Wireless > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	Select **Enable** to activate wireless LAN scheduling on your Device.
WLAN status	Select **On** or **Off** to enable or disable the wireless LAN.
Day	Select the day(s) you want to turn the wireless LAN on or off.
Between the following times	Specify the time period during which to apply the schedule. For example, you want the wireless network to be only available during work hours. Check Mon ~ Fri in the day column, and specify 8:00 ~ 18:00 in the time table.

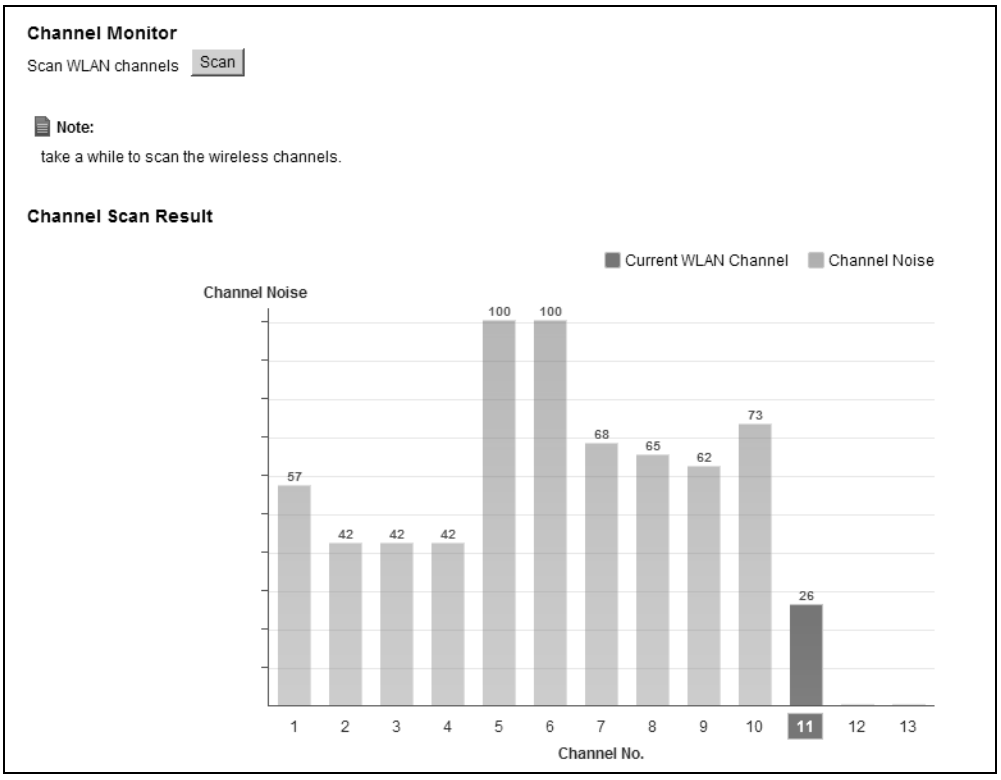
Table 19 Network Setting > Wireless > Scheduling (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.7 The Channel Status Screen

Use the **Channel Status** screen to scan wireless LAN channel noises and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Click **Scan** to scan the wireless LAN channels. You can view the results in the **Channel Scan Result** section.

Figure 30 Network Setting > Wireless > Channel Status



6.8 Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

6.8.1 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the Device's web configurator.

Table 20 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the Device does, it cannot communicate with the Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

6.8.2 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random

and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

6.8.2.1 SSID

Normally, the Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

6.8.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

6.8.2.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

6.8.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 6.8.2.3 on page 111 for information about this.)

Table 21 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

6.8.3 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

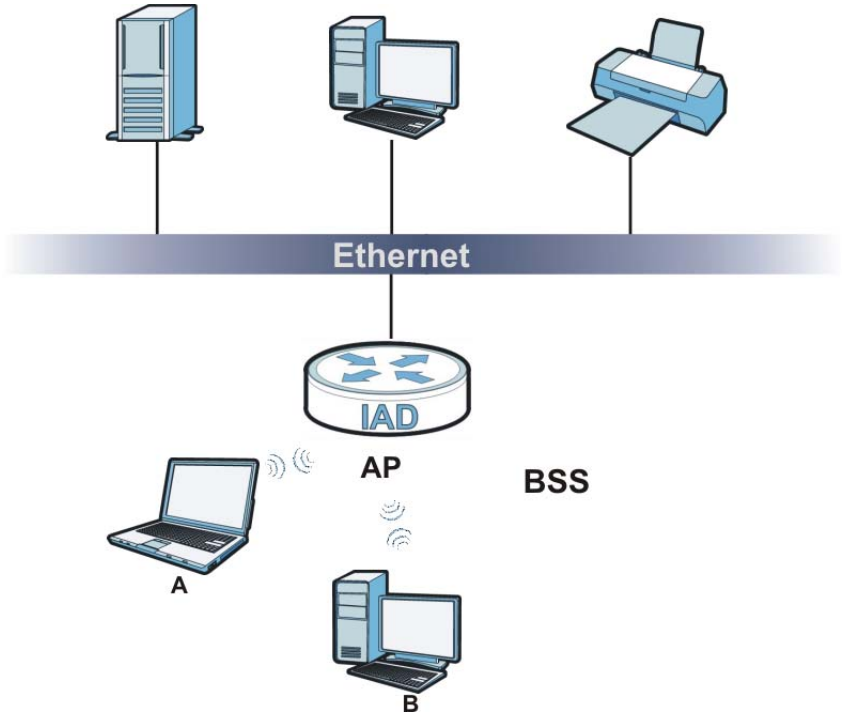
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

6.8.4 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 31 Basic Service set



6.8.5 WiFi Protected Setup (WPS)

Your Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

6.8.5.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Device, see Section 6.4 on page 105).
3. Press the button on one of the devices (it doesn't matter which). For the Device you must press the WPS button for more than three seconds.
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

6.8.5.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
3. Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the Device, see Section 6.4 on page 105).
4. Enter the client's PIN in the AP's configuration interface.

5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

6 Start WPS on both devices within two minutes.

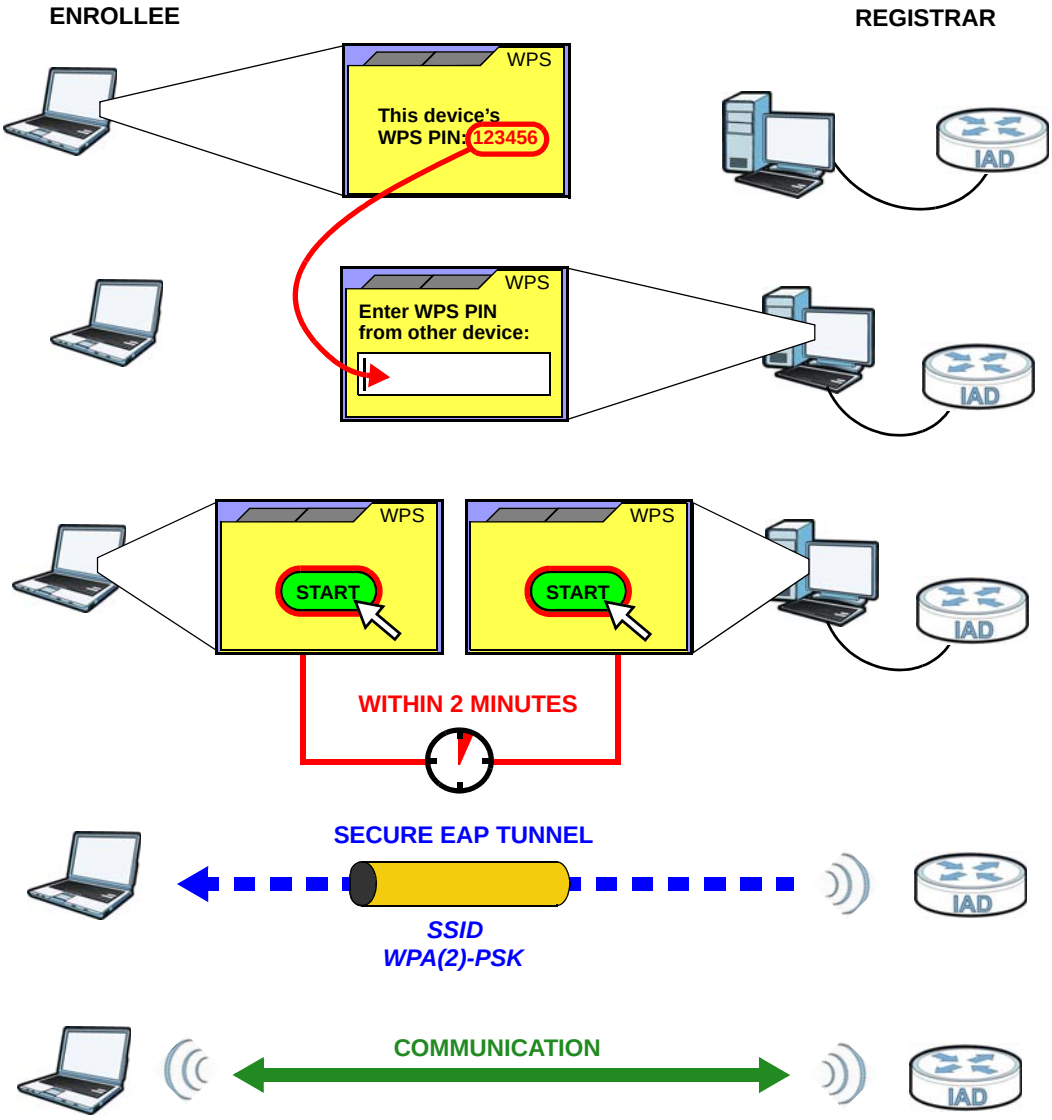
7 Use the configuration utility to activate WPS, not the push-button on the device itself.

8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 32 Example WPS Process: PIN Method

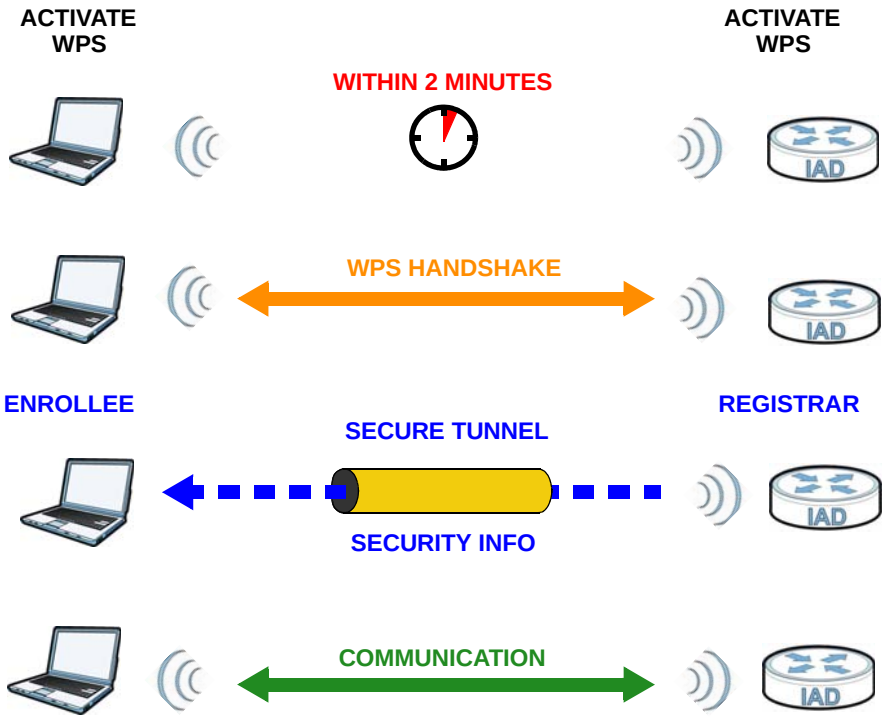


6.8.5.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 33 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS

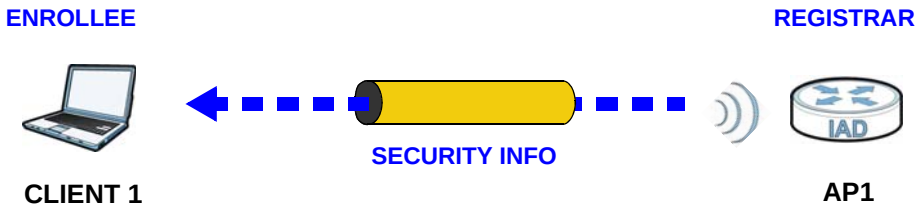
connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

6.8.5.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

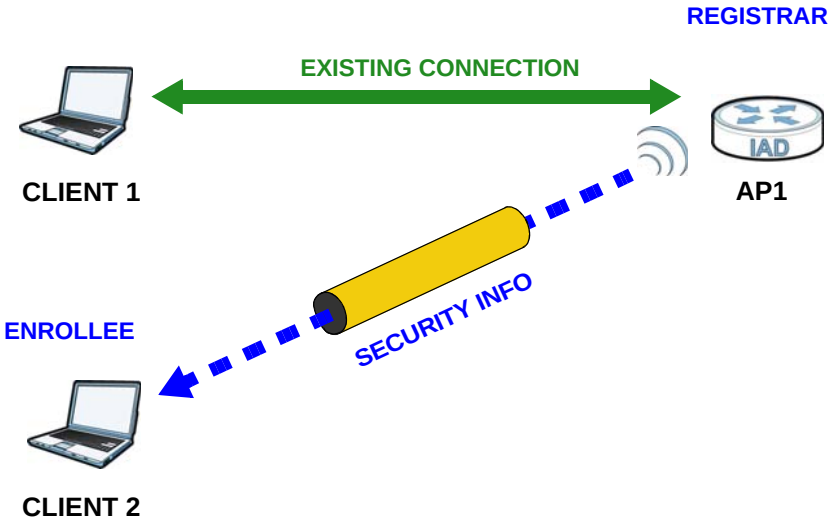
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 34 WPS: Example Network Step 1



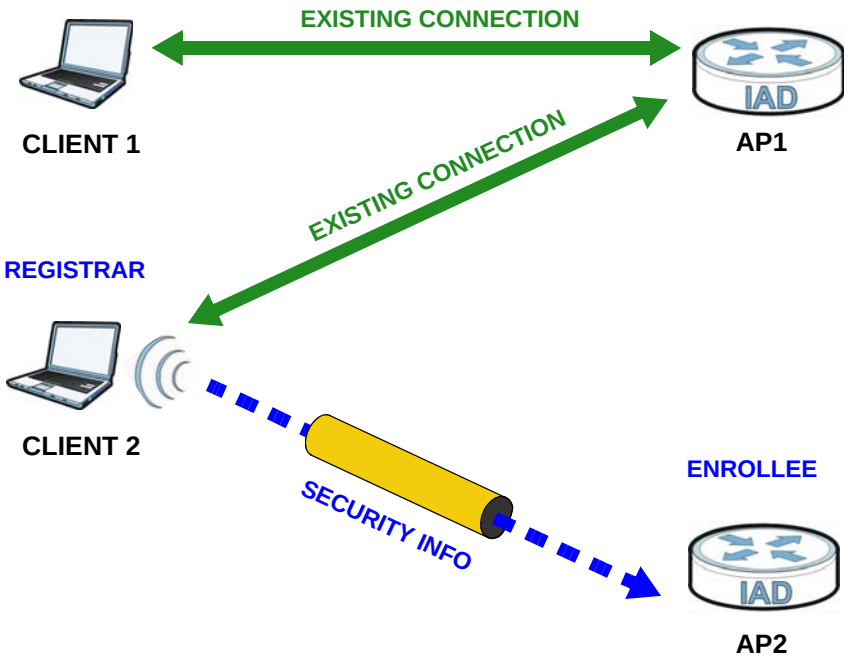
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 35 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 36 WPS: Example Network Step 3



6.8.5.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

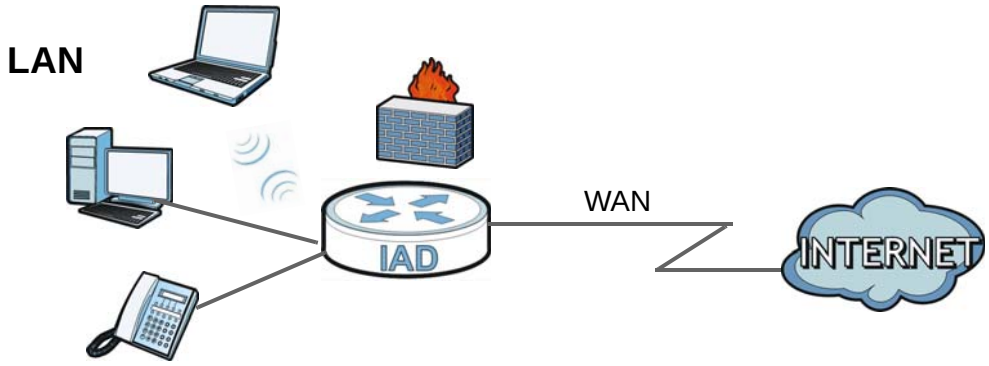
7

Home Networking

7.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.



7.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 7.2 on page 124).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 7.3 on page 125).
- Use the **UPnP** screen to enable UPnP (Section 7.4 on page 127).
- Use the **File Sharing** screen to enable file-sharing server (Section 7.5 on page 127).
- Use the **Media Server** screen to enable or disable the sharing of media files (Section 7.6 on page 130).
- Use the **Printer Server** screen to enable the print server (Section 7.7 on page 131).

7.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

7.1.2.1 About LAN

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Device unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

7.1.2.2 About UPnP

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See Section 7.9 on page 136 for examples of installing and using UPnP.

7.1.2.3 About File Sharing

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the Device is given a folder, called a “share”. If a USB hard drive connected to the Device has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your Device supports File Allocation Table (FAT) and FAT32.

Common Internet File System

The Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

7.1.2.4 About Printer Server

Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

TCP/IP

TCP/IP (Transmission Control Protocol/ Internet Protocol) is a set of communications protocols that most of the Internet runs on.

Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

Supported OSs

Your operating system must support TCP/IP ports for printing and be compatible with the RAW (port 9100) protocol.

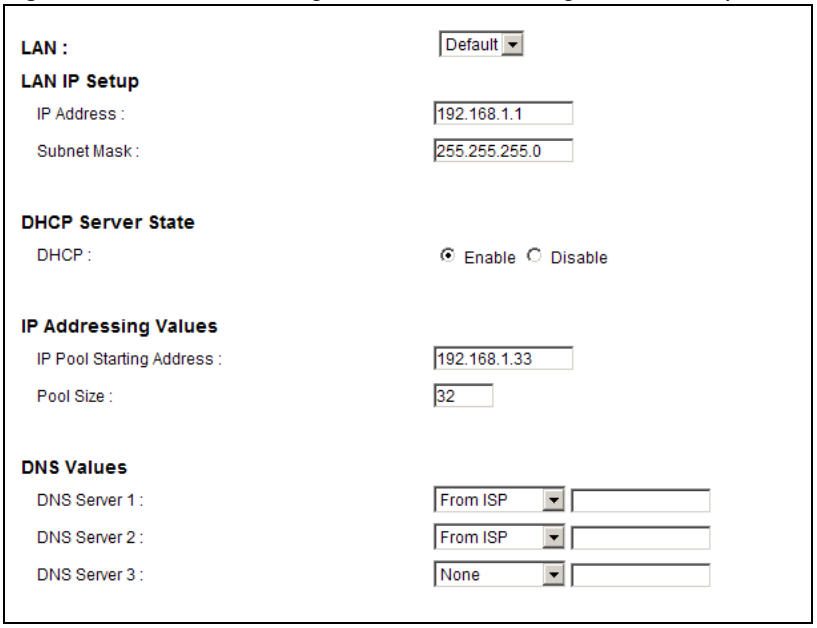
The following OSs support Device's printer sharing feature.

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X.

7.2 The LAN Setup Screen

Click **Network Setting > Home Networking** to open the **LAN Setup** screen. Use this screen to set the Local Area Network IP address and subnet mask of your Device and configure the DNS server information that the Device sends to the DHCP client devices on the LAN.

Figure 37 Network Setting > Home Networking > LAN Setup



The following table describes the fields in this screen.

Table 22 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	

Table 22 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DHCP	Select **Enable** to have your Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN. When DHCP is used, the following fields need to be set.
IP Addressing Values	
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DNS Values	
DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Device's WAN IP address). Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.3 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

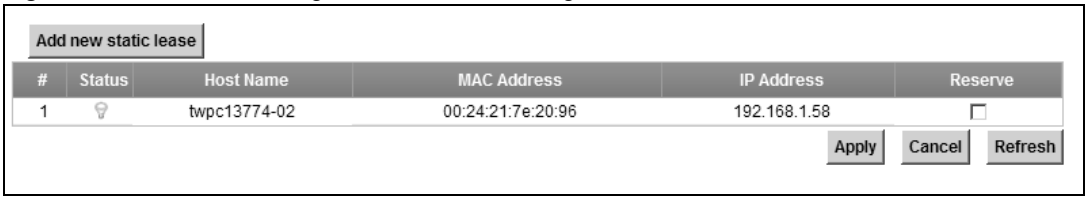
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

7.3.1 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

Use this screen to change your Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 38 Network Setting > Home Networking > Static DHCP


Add new static lease
Status Host Name MAC Address IP Address Reserve
1 twpc13774-02 00:24:21:7e:20:96 192.168.1.58
Apply Cancel Refresh

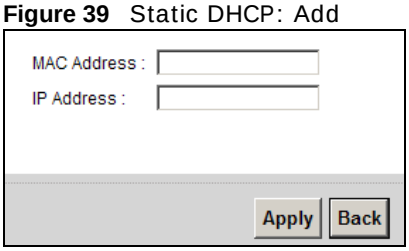
The following table describes the labels in this screen.

Table 23 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the Device.
Host Name	This field displays the client host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.
Refresh	Click **Refresh** to reload the DHCP table.

If you click **Add new static lease** in the **Static DHCP** screen, the following screen displays.

Figure 39 Static DHCP: Add



The following table describes the labels in this screen.

Table 24 Static DHCP: Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of a computer on your LAN.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.

Table 24 Static DHCP: Add (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

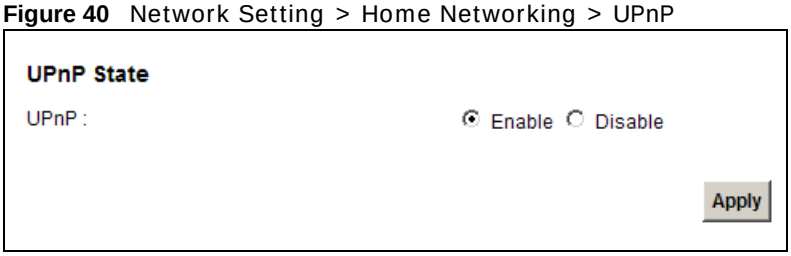
7.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See page 136 for more information on UPnP.

Use the following screen to configure the UPnP settings on your Device. Click **Network Setting > Home Networking > Static DHCP > UPnP** to display the screen shown next.

Figure 40 Network Setting > Home Networking > UPnP



The following table describes the labels in this screen.

Table 25 Network Settings > Home Networking > UPnP

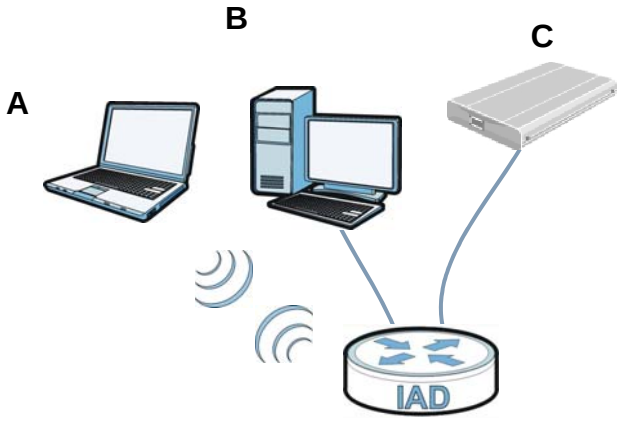
LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Device's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save your changes.

7.5 The File Sharing Screen

You can share files on a USB memory stick or hard drive connected to your Device with users on your network.

The following figure is an overview of the Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Device.

Figure 41 File Sharing Overview



The Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

7.5.1 Before You Begin

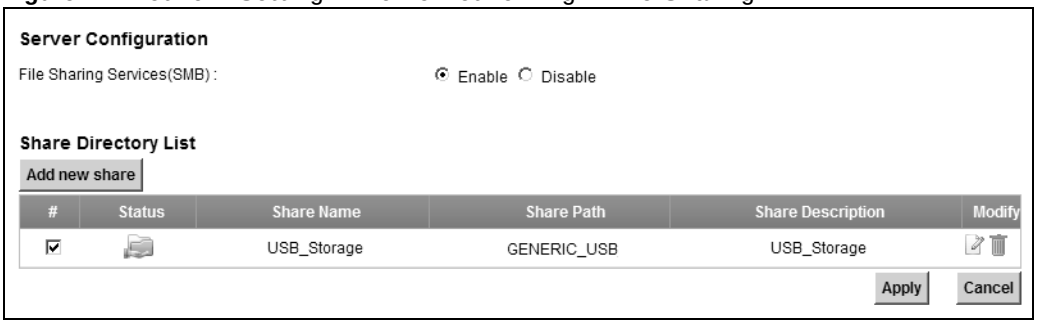
Make sure the Device is connected to your network and turned on.

1. Connect the USB device to one of the Device's USB ports. Make sure the Device is connected to your network.
2. The Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the Device, see the troubleshooting for suggestions.

Use this screen to set up file sharing using the Device. To access this screen, click **Network Setting > Home Networking > File Sharing**.

Figure 42 Network Setting > Home Networking > File Sharing



Each field is described in the following table.

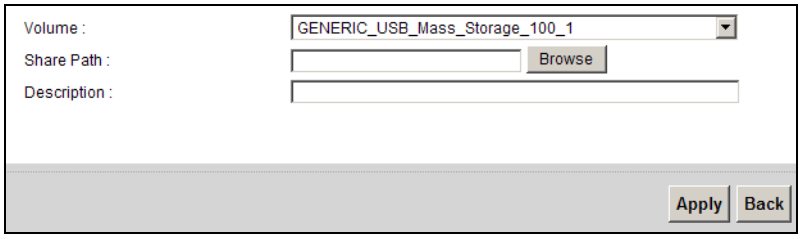
Table 26 Network Setting > Home Networking > File Sharing

LABEL	DESCRIPTION
Server Configuration	
File Sharing Services (SMB)	Select **Enable** to activate file sharing through the Device.
Add new share	Click this to set up a new share on the Device.
#	Select the check box to make the share available to the network. Otherwise, clear this.
Status	This shows whether or not the share is available for sharing.
Share Name	This field displays the share name on the Device.
Share Path	This field displays the path for the share directories (folders) on the Device. These are the directories (folders) on your USB storage device.
Share Description	This field displays information about the share.
Modify	Click the **Edit** icon to change the settings of an existing share. Click the **Delete** icon to delete this share in the list.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.5.2 Add/Edit File Sharing

Use this screen to set up a new share or edit an existing share on the Device. Click **Add new share** in the **File Sharing** screen or click the **Edit** icon next to an existing share.

Figure 43 File Sharing: Add/Edit



Each field is described in the following table.

Table 27 File Sharing: Add/Edit

LABEL	DESCRIPTION
Volume	Select the volume in the USB storage device that you want to add as a share in the Device. This field is read-only when you are editing the share.
Share Path	Manually enter the file path for the share, or click the **Browse** button and select the folder that you want to add as a share. This field is read-only when you are editing the share.
Description	You can either enter a short description of the share, or leave this field blank.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

7.6 The Media Server Screen

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your Device (without having to copy them to another computer). The Device can function as a DLNA-compliant media server. The Device streams files to DLNA-compliant media clients (like Windows Media Player). The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

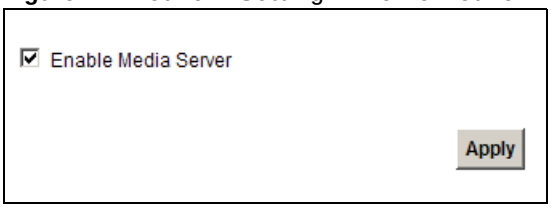
The Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

To change your Device's media server settings, click **Network Setting > Home Networking > Media Server**. The screen appears as shown.

Figure 44 Network Setting > Home Networking > Media Server



The following table describes the labels in this menu.

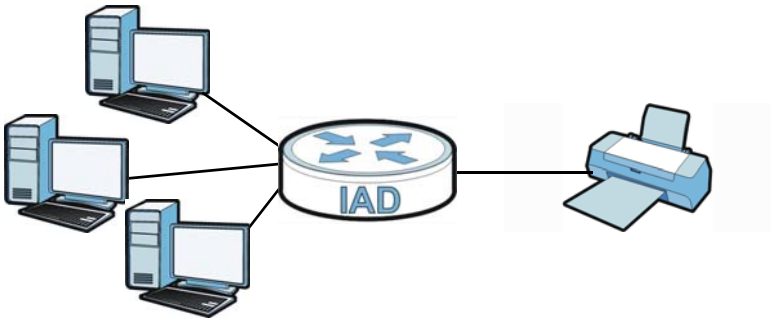
Table 28 Network Setting > Home Networking > Media Server

LABEL	DESCRIPTION
Enable Media Server	Check this to have the Device function as a DLNA-compliant media server. Enable the media server to let (DLNA-compliant) media clients on your network play media files located in the shares.
Apply	Click **Apply** to save your changes.

7.7 The Printer Server Screen

The Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the Device and then configuring a TCP/IP port on the computers connected to your network.

Figure 45 Sharing a USB Printer



7.7.1 Before You Begin

To configure the print server you need the following:

- Your Device must be connected to your computer and any other devices on your network. The USB printer must be connected to your Device.
- A USB printer with the driver already installed on your computer.
- The computers on your network must have the printer software already installed before they can create a TCP/IP port for printing via the network. Follow your printer manufacturers instructions on how to install the printer software on your computer.

Note: Your printer's installation instructions may ask that you connect the printer to your computer. Connect your printer to the Device instead.

Use this screen to enable or disable sharing of a USB printer via your Device.

To access this screen, click **Network Setting > Home Networking > Printer Server**.

Figure 46 Network Setting > Home Networking > Printer Server

The following table describes the labels in this menu.

Table 29 Network Setting > Home Networking > Print Server

LABEL	DESCRIPTION
Printer Server	Select **Enable** to have the Device share a USB printer.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

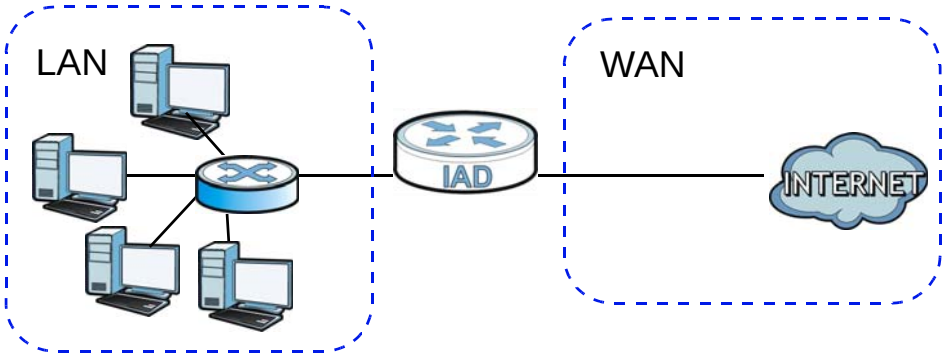
7.8 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

LANs, WANs and the Device

The actual physical connection determines whether the Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 47 LAN and WAN IP Addresses



DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Device as a DHCP server or disable it. When configured as a server, the Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

LAN TCP/IP

The Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

Device Print Server Compatible USB Printers

The following is a list of USB printer models compatible with the Device print server.

Table 30 Compatible USB Printers

BRAND	MODEL
Brother	MFC7420
CANON	BJ F9000
CANON	i320
CANON	PIXMA MP450
CANON	PIXMA MP730
CANON	PIXMA MP780
CANON	PIXMA MP830
CANON	PIXUS ip2500
CANON	PIXMA ip4200
CANON	PIXMA ip5000
CANON	PIXUS 990i
EPSON	CX3500
EPSON	CX3900
EPSON	EPL-5800
EPSON	EPL-6200L
EPSON	LP-2500
EPSON	LP-8900
EPSON	RX 510
EPSON	RX 530
EPSON	Stylus 830U
EPSON	Stylus 1270
EPSON	Stylus C43UX
EPSON	Stylus C60
EPSON	Stylus Color 670
HP	Deskjet 5550
HP	Deskjet 5652
HP	Deskjet 830C
HP	Deskjet 845C
HP	Deskjet 1125C
HP	Deskjet 1180C

Table 30 Compatible USB Printers (continued)

BRAND	MODEL
HP	Deskjet 1220C
HP	Deskjet F4185
HP	Laserjet 1022
HP	Laserjet 1200
HP	Laserjet 2200D
HP	Laserjet 2420
HP	Color Laserjet 1500L
HP	Laserjet 3015
HP	Officejet 4255
HP	Officejet 5510
HP	Officejet 5610
HP	Officejet 7210
HP	Officejet Pro L7380
HP	Photosmart 2610
HP	Photosmart 3110
HP	Photosmart 7150
HP	Photosmart 7830
HP	Photosmart C5280
HP	Photosmart D5160
HP	PSC 1350
HP	PSC 1410
IBM	Infoprint 1332
LEXMARK	Z55
LEXMARK	Z705
OKI	B4350
SAMSUNG	ML-1710
SAMSUNG	SCX-4016

7.9 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

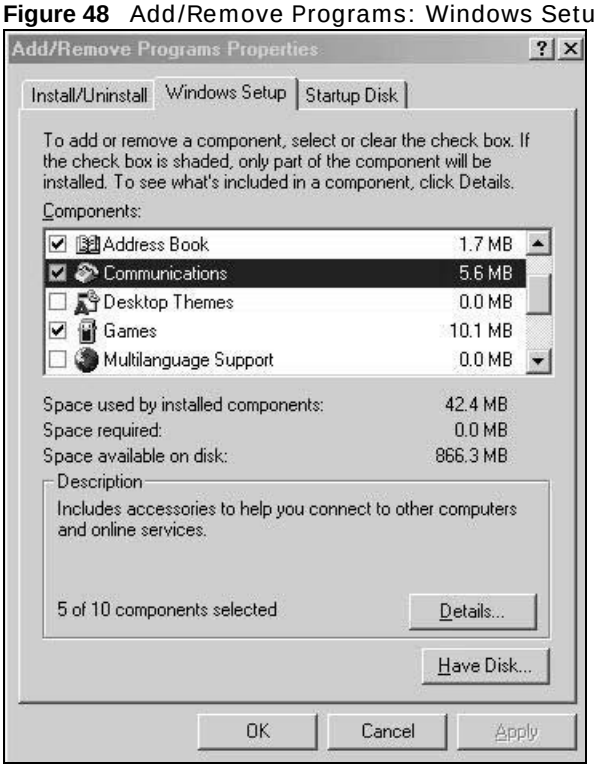
Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

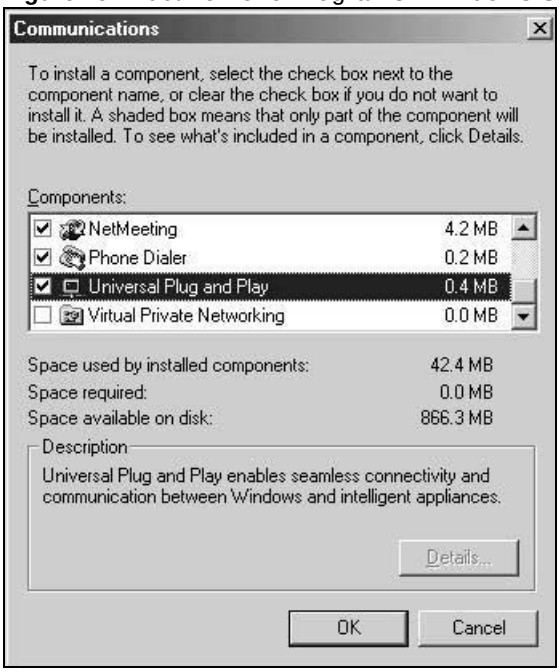
2 Click the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 48 Add/Remove Programs: Windows Setup: Communication


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Games 10.1 MB
Multilanguage Support 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 49 Add/Remove Programs: Windows Setup: Communication: Components


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

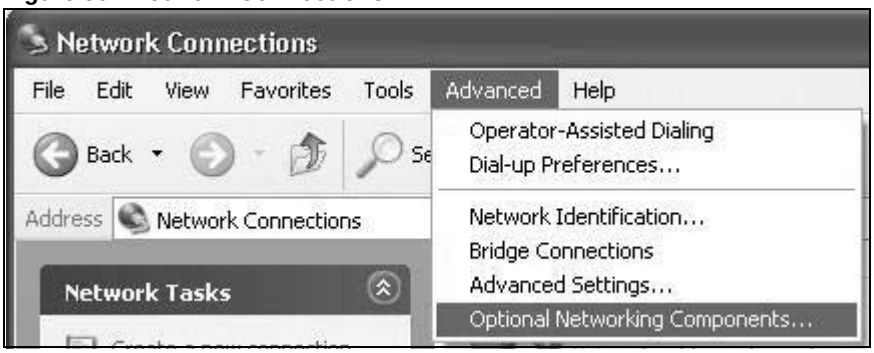
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

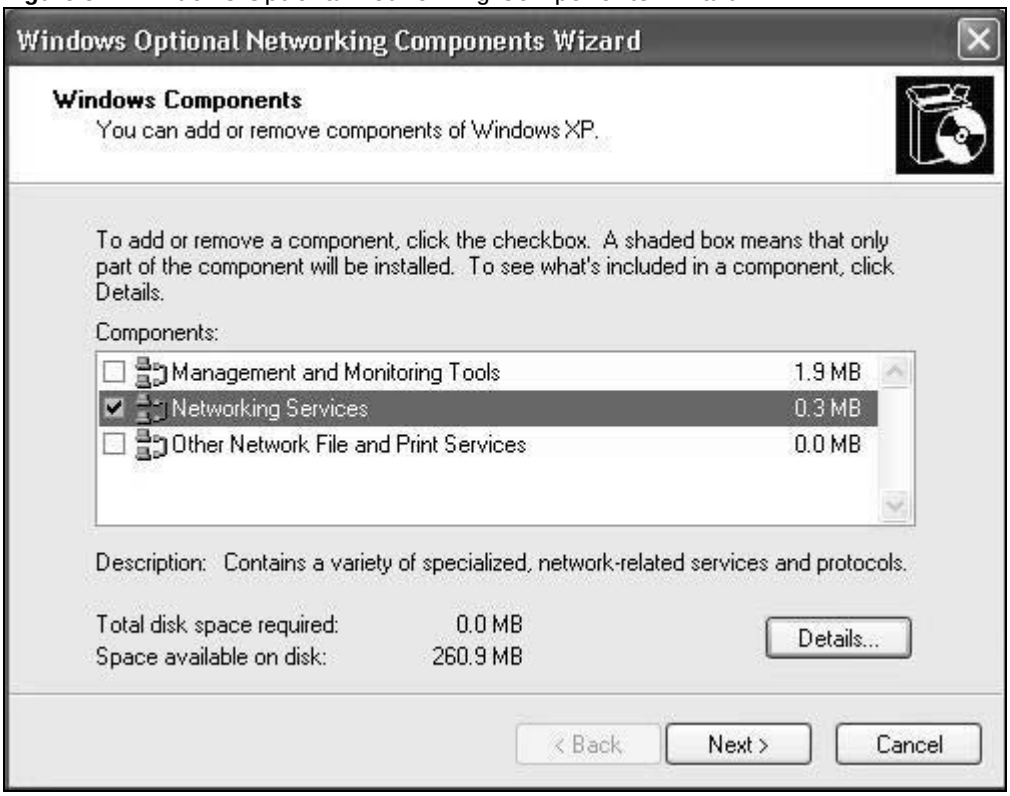
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 50 Network Connections



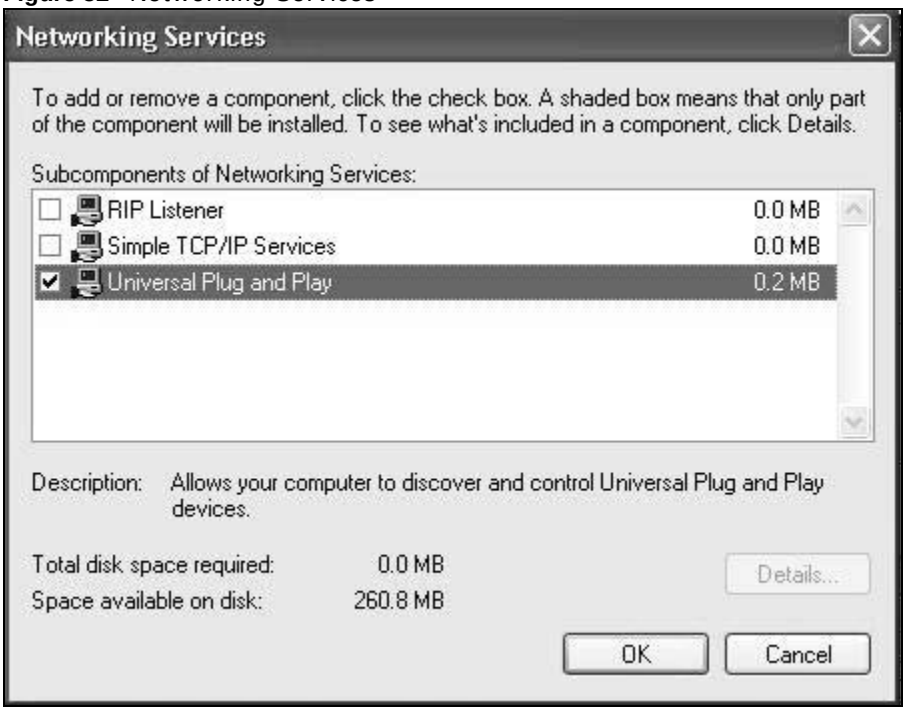
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 51 Windows Optional Networking Components Wizard


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 52 Networking Services


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

7.10 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the Device.

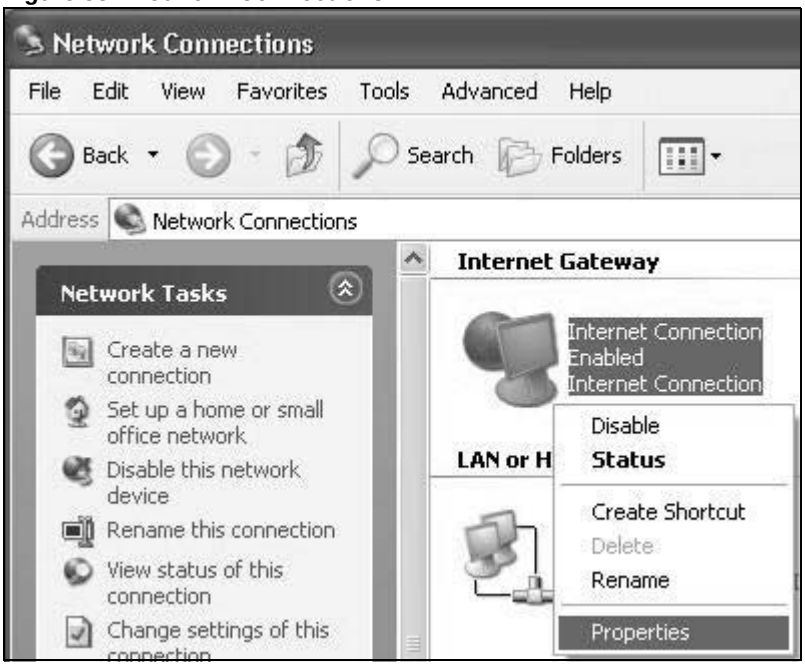
Make sure the computer is connected to a LAN port of the Device. Turn on your computer and the Device.

Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

Figure 53 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 54 Internet Connection Properties

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 55 Internet Connection Properties: Advanced Settings

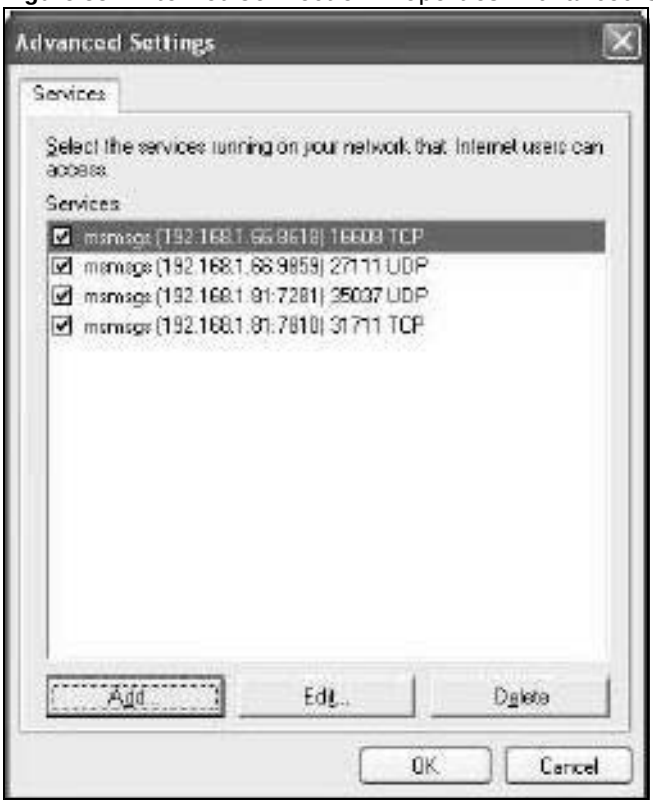
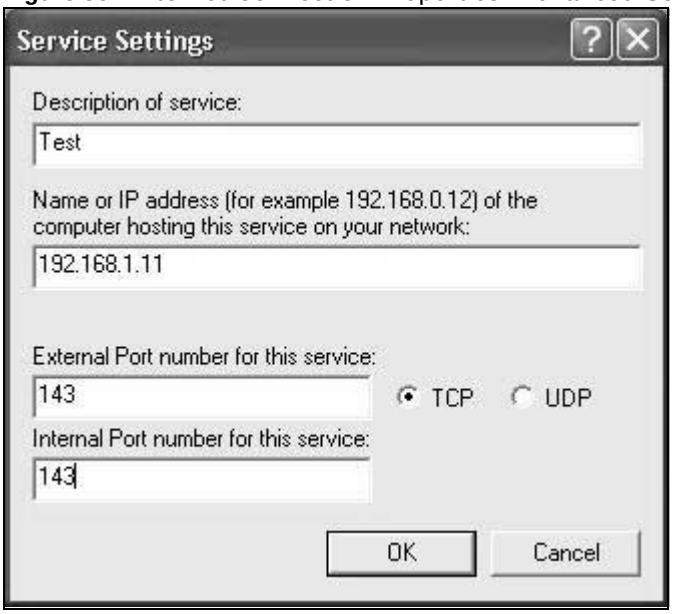


Figure 56 Internet Connection Properties: Advanced Settings: Add



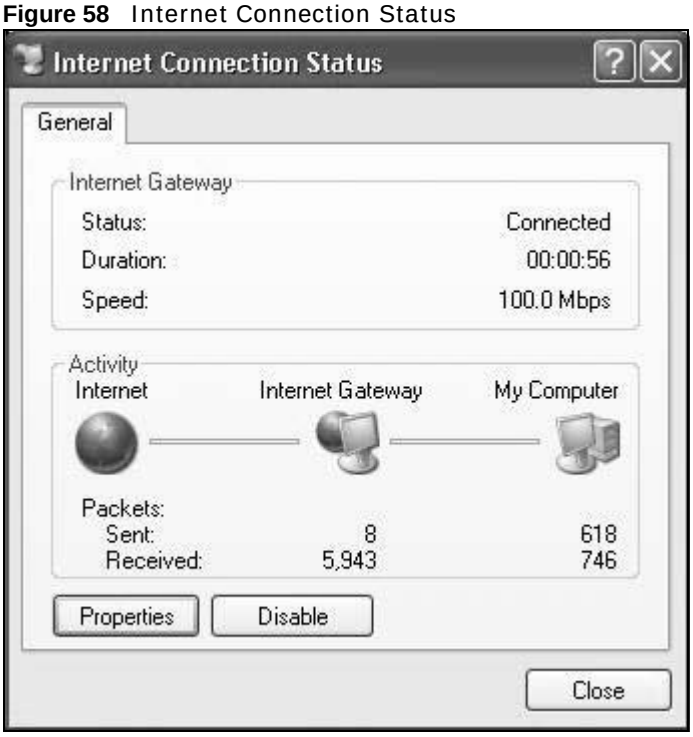
5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 57 System Tray Icon

7 Double-click on the icon to display your current Internet connection status.

Figure 58 Internet Connection Status



Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the Device without finding out the IP address of the Device first. This comes helpful if you do not know the IP address of the Device.

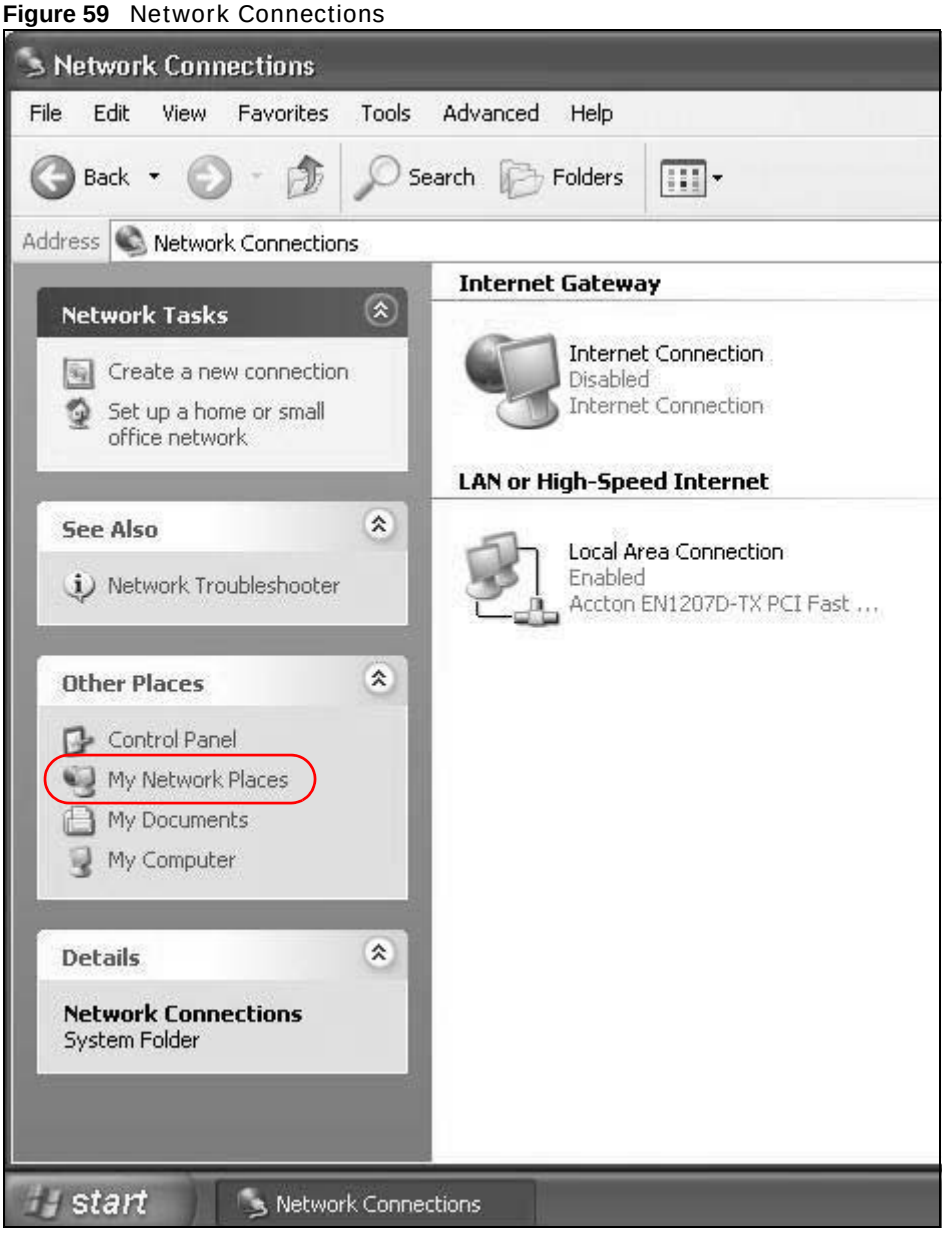
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

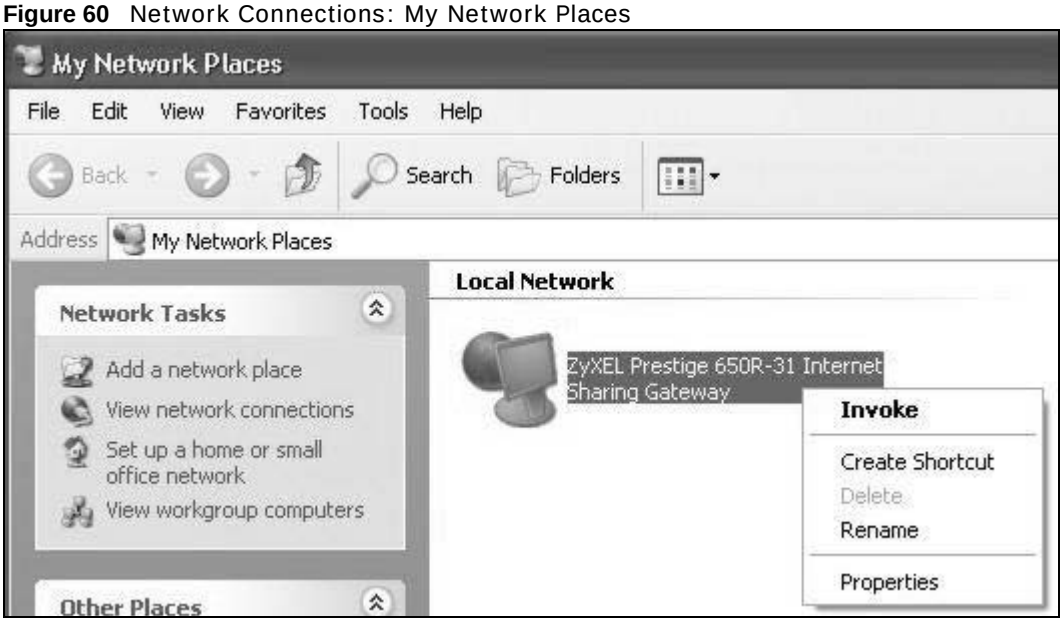
Figure 59 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your Device and select **Invoke**. The web configurator login screen displays.

Figure 60 Network Connections: My Network Places



6 Right-click on the icon for your Device and select **Properties**. A properties window displays with basic information about the Device.

Figure 61 Network Connections: My Network Places: Properties: Example

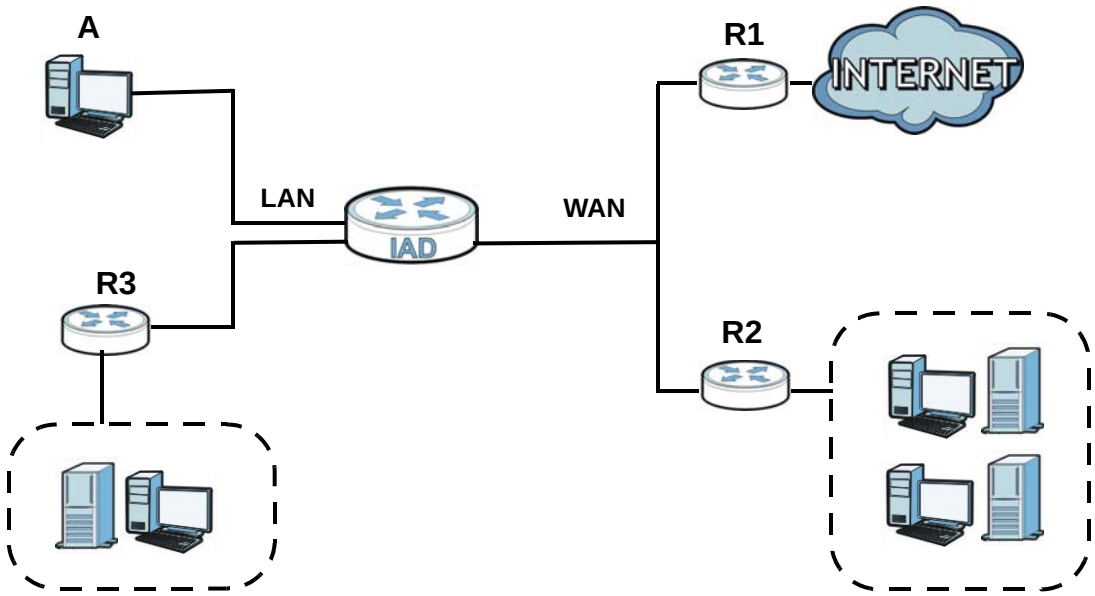
8 Routing

8.1 Overview

The Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Device's LAN interface. The Device routes most traffic from **A** to the Internet through the Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

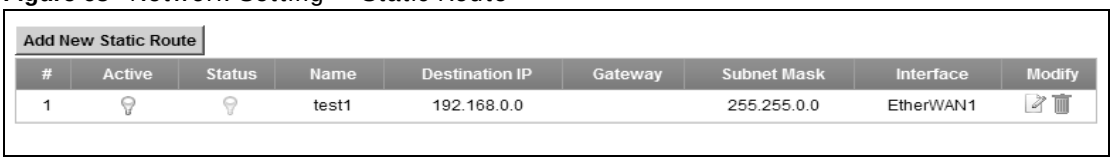
Figure 62 Example of Static Routing Topology



8.2 Configuring Static Route

Use this screen to view and configure IP static routes on the Device. Click **Network Setting > Static Route** to open the following screen.

Figure 63 Network Setting > Static Route


Add New Static Route
Active Status Name Destination IP Gateway Subnet Mask Interface Modify
1 test1 192.168.0.0 255.255.0.0 EtherWAN1

The following table describes the labels in this screen.

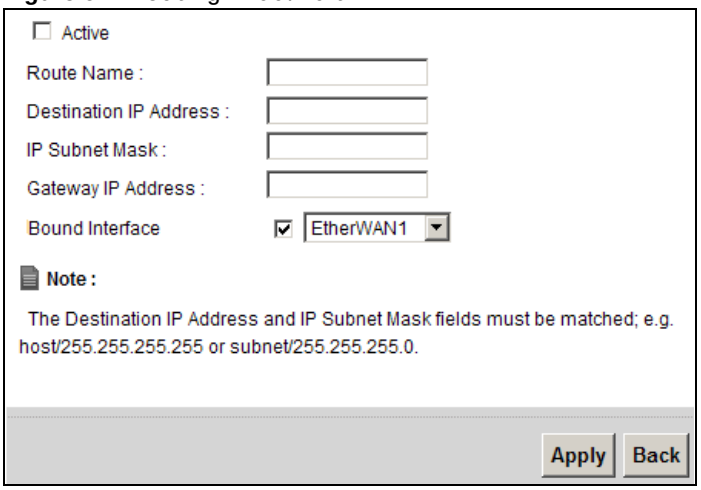
Table 31 Network Setting > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Device.
#	This is the number of an individual static route.
Active	This indicates whether the rule is active or not. A yellow bulb signifies that this static route is active. A gray bulb signifies that this static route is not active.
Status	This shows whether the static route is currently in use or not. A yellow bulb signifies that this static route is in use. A gray bulb signifies that this static route is not in use.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the Device. Click the **Delete** icon to remove a static route from the Device.

8.2.1 Add/Edit Static Route

Click **add new Static Route** in the **Routing** screen or click the **Edit** icon next to a rule. The following screen appears. Use this screen to configure the required information for a static route.

Figure 64 Routing: Add/Edit



The following table describes the labels in this screen.

Table 32 Routing: Add/Edit

LABEL	DESCRIPTION
Active	Click this to activate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Gateway IP Address**, enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Bound Interface	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Bound Interface**, select the check box and choose an interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **Broadband** screen.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

9

Quality of Service (QoS)

9.1 Overview

This chapter discusses the Device's **QoS** screens. Use these screens to set up your Device to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. QoS allows the Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

The Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

Note: The Device has built-in configurations for Voice over IP (IP). The Quality of Service (QoS) feature does not affect VoIP traffic.

- See Section 9.6 on page 159 for advanced technical information on SIP.

9.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable QoS, set the bandwidth, and allow the Device to automatically assign priority to upstream traffic according to the IEEE 802.1p priority level, IP precedence or packet length (Section 9.2 on page 150).
- Use the **Queue Setup** screen to configure QoS queue assignment (Section 9.3 on page 151).
- Use the **Class Setup** screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow (Section 9.4 on page 153).
- Use the **Monitor** screen to view the Device's QoS-related packet statistics (Section 9.5 on page 158).

9.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

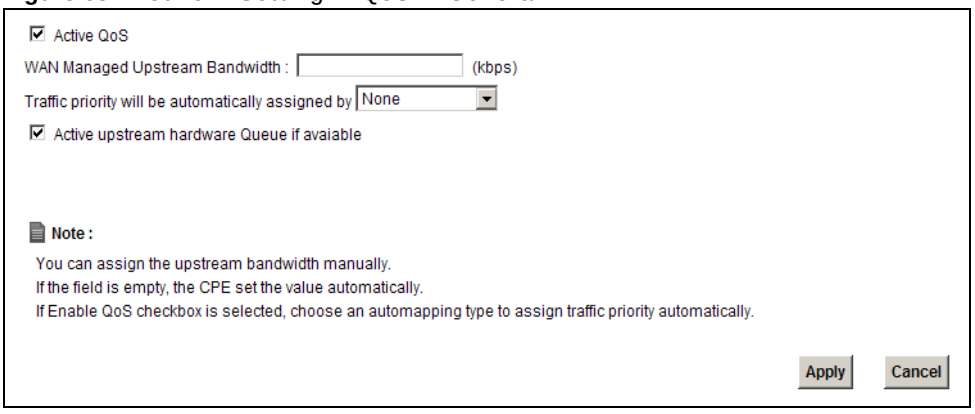
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

9.2 The QoS General Screen

Use this screen to enable or disable QoS, set the bandwidth, and select to have the Device automatically assign priority to upstream traffic according to the IEEE 802.1p priority level, IP precedence or packet length.

Click **Network Setting > QoS** to open the **General** screen.

Figure 65 Network Setting > QoS > General


Active QoS
WAN Managed Upstream Bandwidth :
(kbps)
Traffic priority will be automatically assigned by
None
Active upstream hardware Queue if avaiable
Note :
You can assign the upstream bandwidth manually.
If the field is empty, the CPE set the value automatically.
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.
Apply
Cancel

The following table describes the labels in this screen.

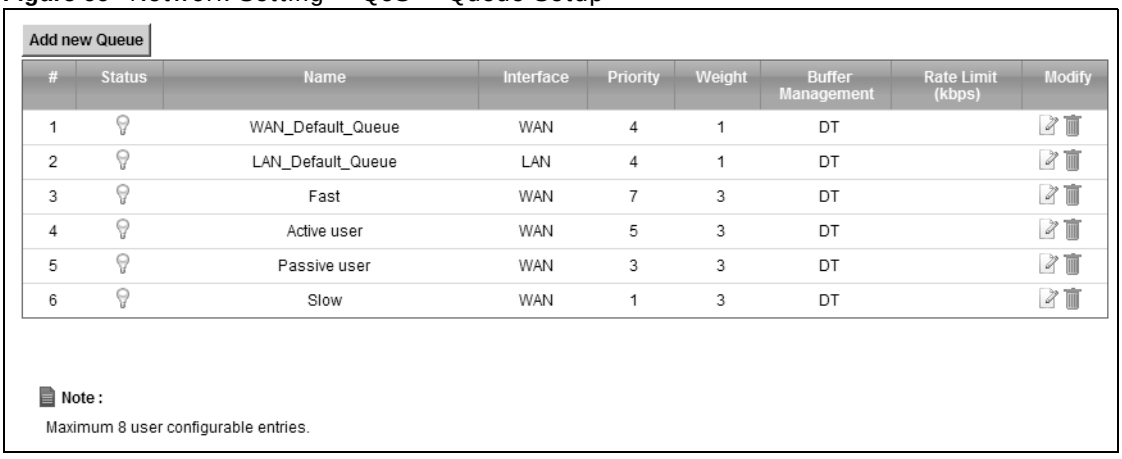
Table 33 Network Setting > QoS > General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
WAN Managed Upstream Bandwidth	Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 1000 kbps if your Internet connection has an upstream transmission speed of 1 Mbps. Setting this number higher than the interface's actual transmission speed will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. If you set this number lower than the interface's actual transmission speed, the Device will not use some of the interface's available bandwidth. Leave this field blank to have the Device set this value automatically.
Traffic priority will be automatically assigned by	These fields are ignored if upstream traffic matches a class you configured in the **Class Setup** screen. If you select **Ethernet Priority**, **IP Precedence** or **Packet Length** and traffic does not match a class configured in the **Class Setup** screen, the Device assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence or packet length. See Section 9.6.1 on page 159 for more information.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

9.3 The Queue Setup Screen

Use this screen to configure QoS queue assignment. Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Figure 66 Network Setting > QoS > Queue Setup


Add new Queue
Status Name Interface Priority Weight Buffer Management Rate Limit (kbps) Modify
1 WAN_Default_Queue WAN 4 1 DT
2 LAN_Default_Queue LAN 4 1 DT
3 Fast WAN 7 3 DT
4 Active user WAN 5 3 DT
5 Passive user WAN 3 3 DT
6 Slow WAN 1 3 DT
Note :
Maximum 8 user configurable entries.

The following table describes the labels in this screen.

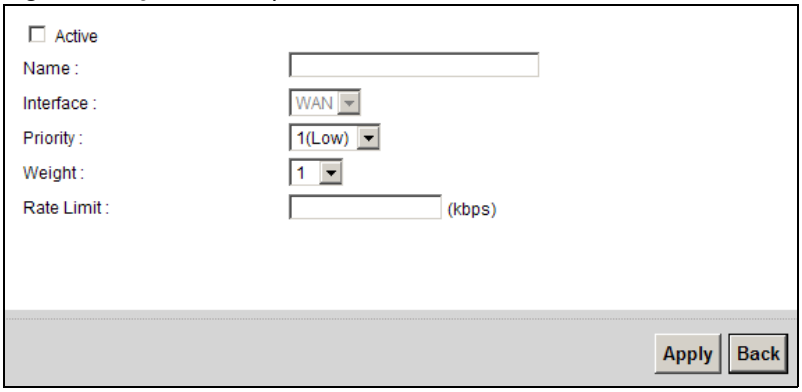
Table 34 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add new Queue	Click this to create a new entry.
#	This is the index number of this entry.
Status	This indicates whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used by the Device.
Rate Limit (kbps)	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

9.3.1 Add/Edit a QoS Queue

Use this screen to configure a queue. Click **Add new queue** in the **Queue Setup** screen or the **Edit** icon next to an existing queue.

Figure 67 Queue Setup: Add/Edit



The following table describes the labels in this screen.

Table 35 Queue Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	This shows the interface of this queue.

Table 35 Queue Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Priority	Select the priority level (from 1 to 7) of this queue. The larger the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 15) of this queue. If two queues have the same priority level, the Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

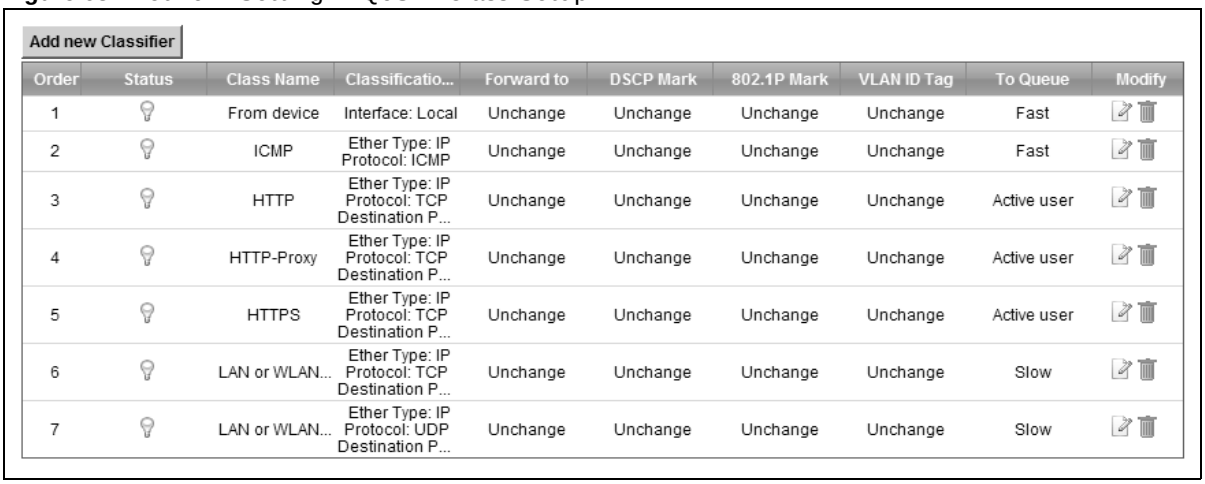
9.4 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Class Setup** to open the following screen.

Figure 68 Network Setting > QoS > Class Setup


Add new Classifier
Order
Status
Class Name
Classificatio...
Forward to
DSCP Mark
802.1P Mark
VLAN ID Tag
To Queue
Modify
1 From device Interface: Local Unchange Unchange Unchange Unchange Fast
2 ICMP Ether Type: IP Protocol: ICMP Unchange Unchange Unchange Unchange Fast
3 HTTP Ether Type: IP Protocol: TCP Destination P... Unchange Unchange Unchange Unchange Active user
4 HTTP-Proxy Ether Type: IP Protocol: TCP Destination P... Unchange Unchange Unchange Unchange Active user
5 HTTPS Ether Type: IP Protocol: TCP Destination P... Unchange Unchange Unchange Unchange Active user
6 LAN or WLAN... Ether Type: IP Protocol: TCP Destination P... Unchange Unchange Unchange Unchange Slow
7 LAN or WLAN... Ether Type: IP Protocol: UDP Destination P... Unchange Unchange Unchange Unchange Slow

The following table describes the labels in this screen.

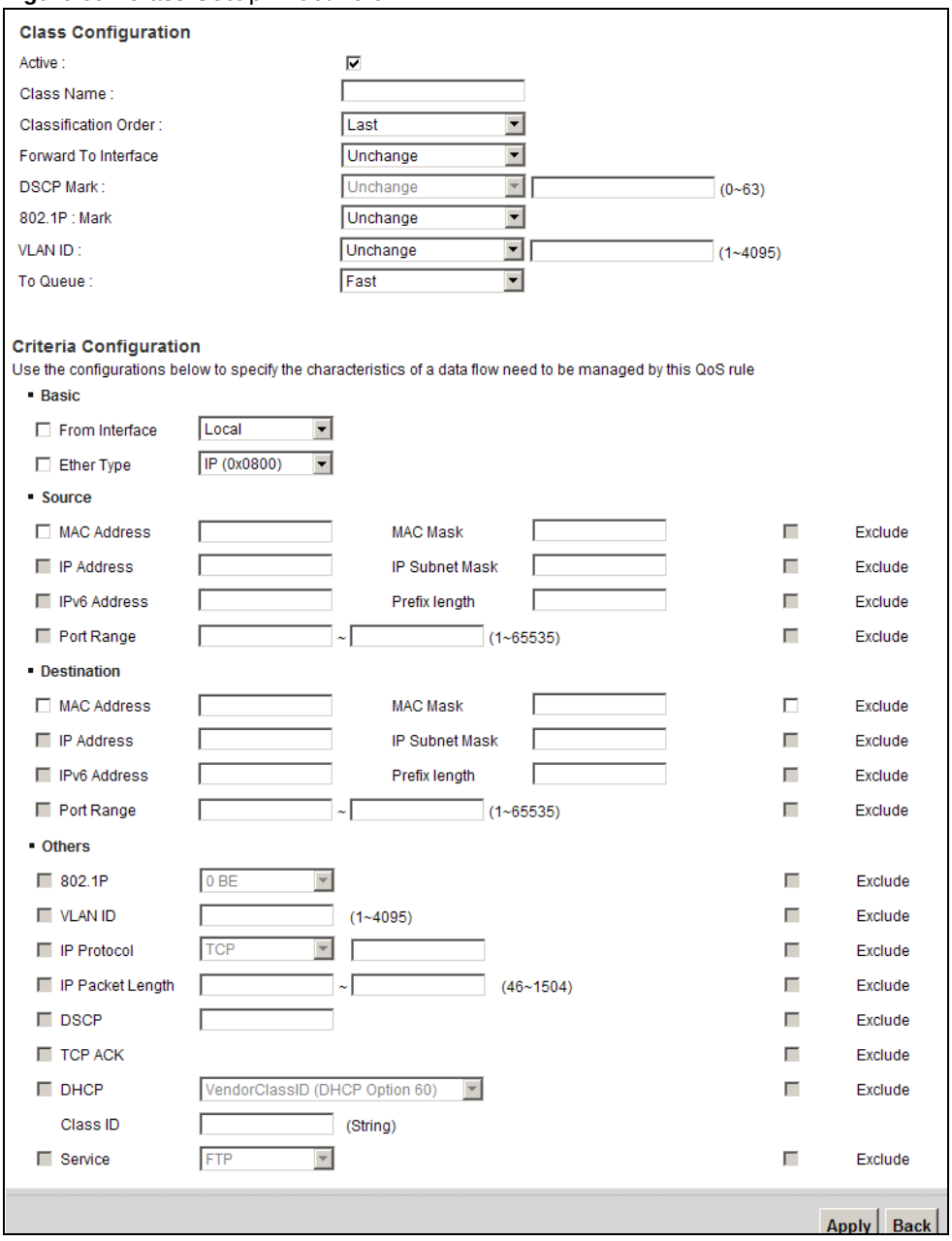
Table 36 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
Order	This field displays the order number of the classifier.
Status	This indicates whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
Forward to	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1p Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

9.4.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to an existing classifier to configure it.

Figure 69 Class Setup: Add/Edit


Class Configuration
Active :
Class Name :
Classification Order : Last
Forward To Interface : Unchange
DSCP Mark : Unchange (0~63)
802.1P : Mark : Unchange
VLAN ID : Unchange (1~4095)
To Queue : Fast
Criteria Configuration
Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule
Basic
From Interface : Local
Ether Type : IP (0x0800)
Source
MAC Address / MAC Mask / Exclude
IP Address / IP Subnet Mask / Exclude
IPv6 Address / Prefix length / Exclude
Port Range (1~65535) / Exclude
Destination
MAC Address / MAC Mask / Exclude
IP Address / IP Subnet Mask / Exclude
IPv6 Address / Prefix length / Exclude
Port Range (1~65535) / Exclude
Others
802.1P : 0 BE / Exclude
VLAN ID (1~4095) / Exclude
IP Protocol : TCP / Exclude
IP Packet Length (46~1504) / Exclude
DSCP / Exclude
TCP ACK / Exclude
DHCP : VendorClassID (DHCP Option 60) / Exclude
Class ID (String)
Service : FTP / Exclude
Apply
Back

The following table describes the labels in this screen.

Table 37 Class Setup: Add/Edit

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable this classifier.

Table 37 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Class Name	Enter a descriptive name of up to 32 printable English keyboard characters, including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the Device forward traffic of this class according to the default routing table.
DSCP Mark	This field is available only when you select the **Ether Type** check box in **Criteria Configuration-Basic** section. If you select **Mark**, enter a DSCP value with which the Device replaces the DSCP field in the packets. If you select **Unchange**, the Device keep the DSCP field in the packets.
802.1p Mark	Select a priority level with which the Device replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the Device keep the 802.1p priority field in the packets.
VLAN ID	If you select **Remark**, enter a VLAN ID number (between 1 and 4095) with which the Device replaces the VLAN ID of the frames. If you select **Remove**, the Device deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the Device treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the Device keep the VLAN ID in the packets.
To Queue	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Criteria Configuration Use the following fields to configure the criteria for traffic classification.	
Basic	
From Interface	Select whether the traffic class comes from the LAN or a wireless interface.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **IPv6**, you need to configure the source or destination IPv6 addres and prefix length. If you select **ARP**, you need to configure the source's MAC address and MAC Mask. If you select **8021Q**, you can configure an 802.1p priority level and VLAN ID in the **Others** section.
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.

Table 37 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
IP Address	If you select **IP** in the **Ether Type** field, select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
IPv6 Address	If you select **IPv6** in the **Ether Type** field, enter the source's IPv6 address.
Prefix length	Enter the source prefix length.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
IPv6 Address	If you select **IPv6** in the **Ether Type** field, enter the destination's IPv6 address.
Prefix length	Enter the destination prefix length.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop down list box."0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field.
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP** or **UDP**. If you select **User defined**, enter the protocol (service type) number.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1504) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.

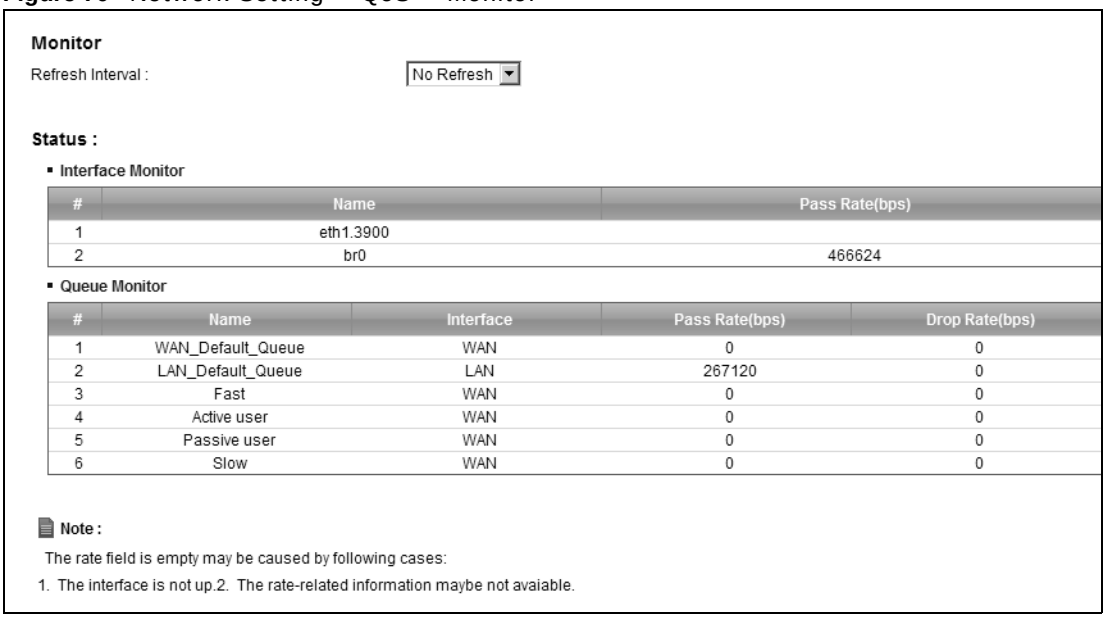
Table 37 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
DHCP	This field is available only when you select **IP** in the **Ether Type** field, and **UDP** in the **IP Protocol** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the **Class ID** of the matched traffic, such as the type of the hardware or firmware. If you select **ClientID (DHCP Option 61)**, enter the **Type** of the matched traffic and **Client ID** of the DHCP client. If you select **User Class ID (DHCP Option 77)**, enter the **User Class Data**, which is a string that identifies the user's category or application type in the matched DHCP packets. If you select **VendorSpecificIntro (DHCP Option 125)**, enter the **Enterprise Number** of the software of the matched traffic and **Vendor Class Data** used by all the DHCP clients.
Service	Select the service classification of the traffic.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

9.5 The QoS Monitor Screen

To view the Device's QoS packet statistics, click **Network Setting > QoS > Monitor**. The screen appears as shown.

Figure 70 Network Setting > QoS > Monitor


Monitor
Refresh Interval :
No Refresh
Status :
Interface Monitor
Name Pass Rate(bps)
1 eth1.3900
2 br0 466624
Queue Monitor
Name Interface Pass Rate(bps) Drop Rate(bps)
1 WAN_Default_Queue WAN 0 0
2 LAN_Default_Queue LAN 267120 0
3 Fast WAN 0 0
4 Active user WAN 0 0
5 Passive user WAN 0 0
6 Slow WAN 0 0
Note :
The rate field is empty may be caused by following cases:
1. The interface is not up.2. The rate-related information maybe not avaiable.

The following table describes the labels in this screen.

Table 38 Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Monitor	
Refresh Interval	Select how often you want the Device to update this screen. Select **No Refresh** to stop refreshing statistics.
Status	
#	This is the index number of the entry.
Name	This shows the name of the WAN interface on the Device.
Pass Rate (bps)	This shows how much traffic (bps) forwarded to this interface are transmitted successfully.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate (bps)	This shows how much traffic (bps) assigned to this queue are transmitted successfully.
Drop Rate (bps)	This shows how much traffic (bps) assigned to this queue are dropped.

9.6 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

9.6.1 IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 39 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.

Table 39 IEEE 802.1p Priority Level and Traffic Type (continued)

PRIORITY LEVEL	TRAFFIC TYPE
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

9.6.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

9.6.3 DiffServ

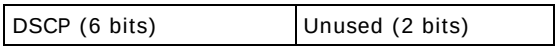
QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

10

Network Address Translation (NAT)

10.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

10.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 10.2 on page 162).
- Use the **DMZ** screen to configure a default server (Section 10.3 on page 165).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use (Section on page 164).
- Use the **Address Mapping** screen to configure the Device's address mapping settings (Section 10.5 on page 166).
- Use the **ALG** screen to enable and disable the SIP (VoIP) ALG in the Device (Section 10.6 on page 168).

10.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See Section 10.7 on page 168 for advanced technical information on NAT.

10.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

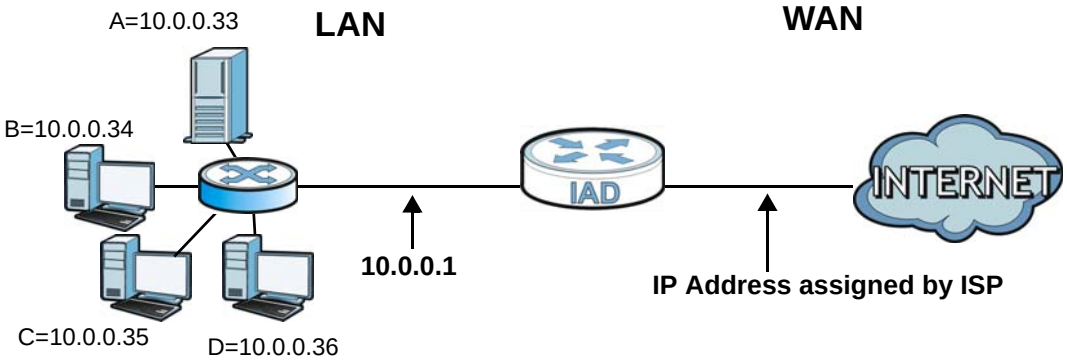
The most often used port numbers and services are shown in Appendix E on page 353. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 10.0.0.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 71 Multiple Servers Behind NAT Example

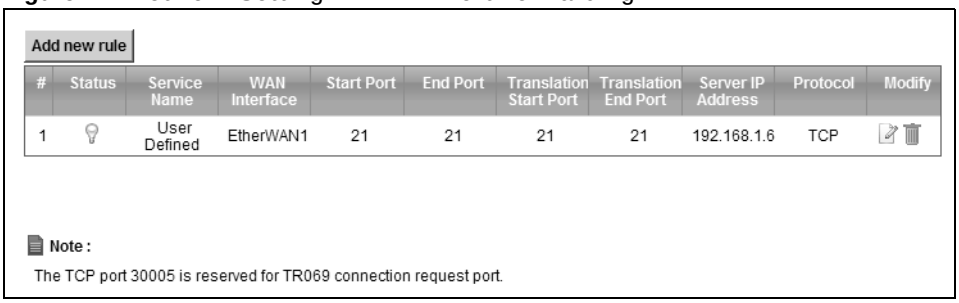


10.2.1 The Port Forwarding Screen

Click **Network Setting > NAT** to open the **Port Forwarding** screen.

See Appendix E on page 353 for port numbers commonly used for particular services.

Figure 72 Network Setting > NAT > Port Forwarding


Add new rule
Status Service Name WAN Interface Start Port End Port Translation Start Port Translation End Port Server IP Address Protocol Modify
1 User Defined EtherWAN1 21 21 21 21 192.168.1.6 TCP
Note :
The TCP port 30005 is reserved for TR069 connection request port.

The following table describes the fields in this screen.

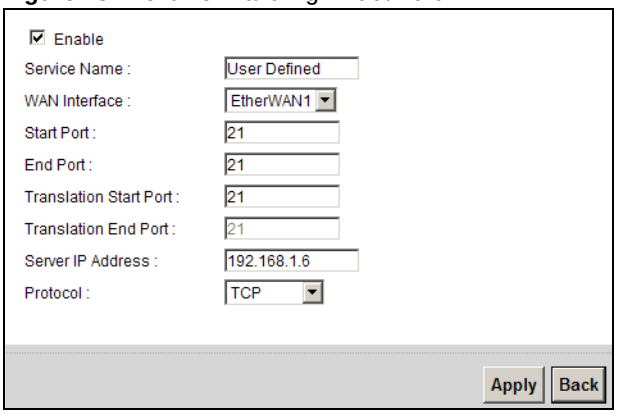
Table 40 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add new rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows **User Defined** if you manually added a service. You can change this by clicking the edit icon.
WAN Interface	This shows the WAN interface through which the service is forwarded.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Server IP Address	This is the server's IP address.
Protocol	This shows the IP protocol supported by this virtual server, whether it is **TCP**, **UDP**, or **TCP/UDP**.
Modify	Click the **Edit** icon to edit the port forwarding rule. Click the **Delete** icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.2.2 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Click **Add new rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

Figure 73 Port Forwarding: Add/Edit



The following table describes the labels in this screen.

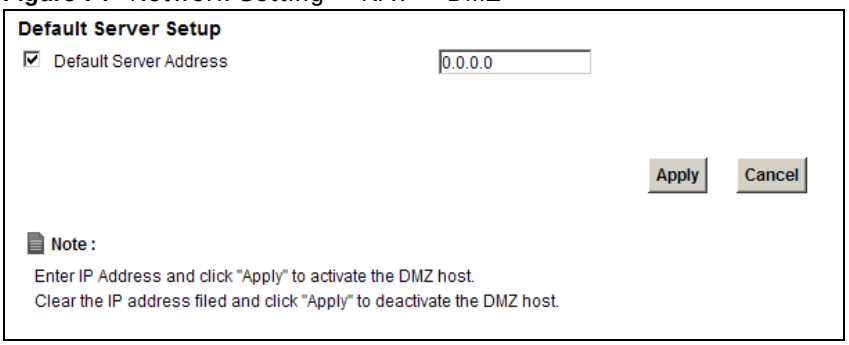
Table 41 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Enable	This is available only in the **Edit** screen. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Translation Start Port	This shows the port number to which you want the Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol Type	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

10.3 The DMZ Screen

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in the **NAT Port Forwarding Setup** screen.

Figure 74 Network Setting > NAT > DMZ


Default Server Setup
Default Server Address
0.0.0.0
Apply
Cancel
Note :
Enter IP Address and click "Apply" to activate the DMZ host.
Clear the IP address filed and click "Apply" to deactivate the DMZ host.

The following table describes the fields in this screen.

Table 42 Network Setting > NAT > DMZ

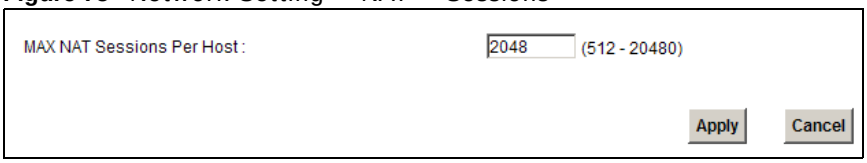
LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen. Note: If you do not assign a **Default Server Address**, the Device discards all packets received for ports that are not specified in the **NAT Port Forwarding** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.4 The Sessions Screen

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use.

Click **Network Setting > NAT > Sessions** to display the following screen.

Figure 75 Network Setting > NAT > Sessions



The following table describes the fields in this screen.

Table 43 Network Setting > NAT > Sessions

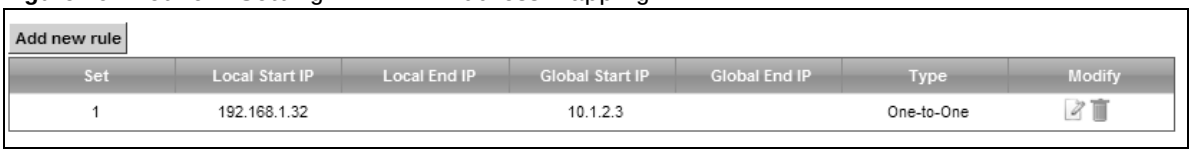
LABEL	DESCRIPTION
MAX NAT Session	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.5 The Address Mapping Screen

Ordering your rules is important because the Device applies the rules in the order that you specify. When a rule matches the current packet, the Device takes the corresponding action and the remaining rules are ignored.

Click **Network Setting > NAT > Address Mapping** to display the following screen.

Figure 76 Network Setting > NAT > Address Mapping



The following table describes the fields in this screen.

Table 44 Network Setting > NAT > Address Mapping

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
Set	This is the index number of the address mapping set.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.

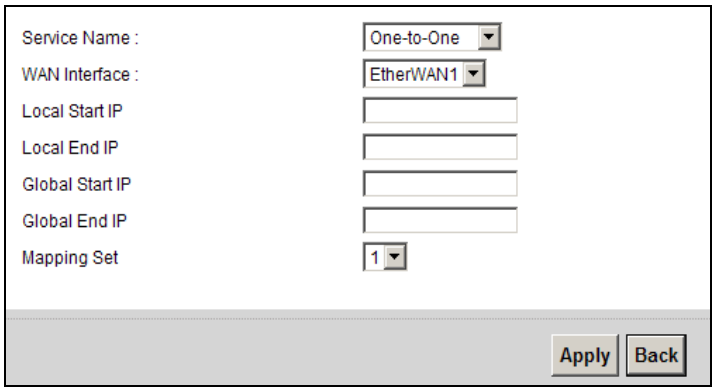
Table 44 Network Setting > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
Type	This is the address mapping type. **One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
Modify	Click the **Edit** icon to go to the screen where you can edit the address mapping rule. Click the **Delete** icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

10.5.1 Add/Edit Address Mapping Rule

To add or edit an address mapping rule, click **Add new rule** or the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 77 Address Mapping: Add/Edit



The following table describes the fields in this screen.

Table 45 Address Mapping: Add/Edit

LABEL	DESCRIPTION
Type	Choose the IP/port mapping type from one of the following. **One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
WAN Interface	Select the WAN interface.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types.

Table 45 Address Mapping: Add/Edit (continued)

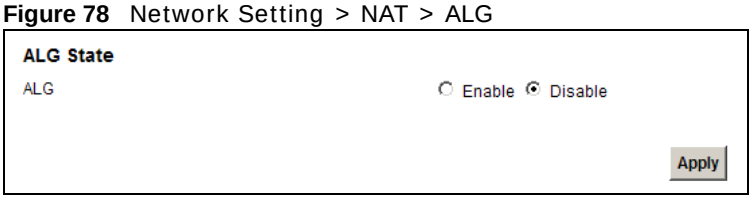
LABEL	DESCRIPTION
Global Start IP	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
MAP Set	Select the number of the mapping set for which you want to configure.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.6 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the Device registers with the SIP register server, the SIP ALG translates the Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Device is behind a SIP ALG.

Use this screen to enable or disable the SIP (VoIP) ALG in the Device. To access this screen, click **Network Setting > NAT > ALG**.

Figure 78 Network Setting > NAT > ALG



The following table describes the fields in this screen.

Table 46 Network Setting > NAT > ALG

LABEL	DESCRIPTION
ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click **Apply** to save your changes.

10.7 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

10.7.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 47 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

10.7.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

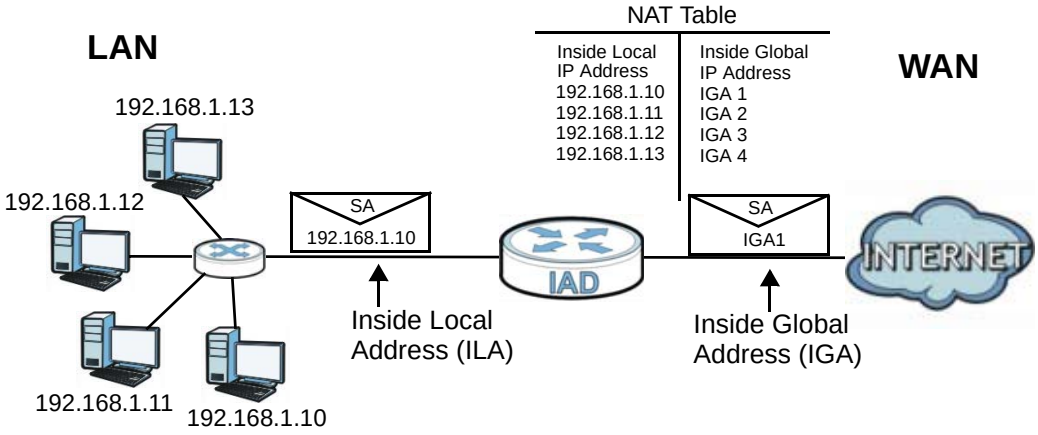
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a Telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

10.7.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The

Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 79 How NAT Works



11

DNS Route

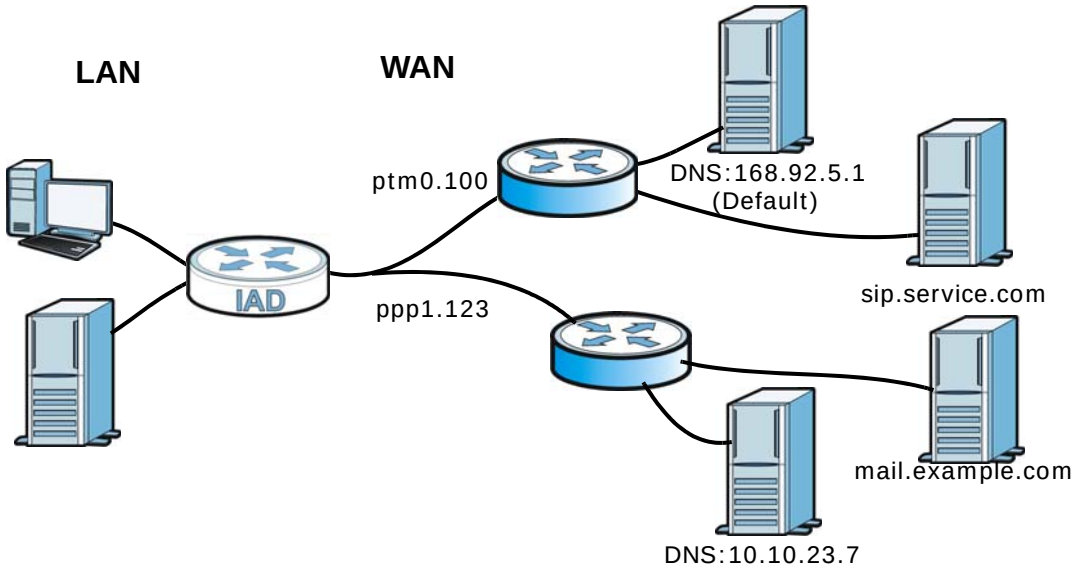
11.1 Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

In the following example, the DNS server 168.92.5.1 obtained from the WAN interface ptm0.100 is set to be the system DNS server. The DNS server 10.10.23.7 is obtained from the WAN interface ppp1.123. You configure a DNS route for *example.com to have the Device forward DNS requests for the domain name mail.example.com through the WAN interface ppp1.123 to the DNS server 10.10.23.7.

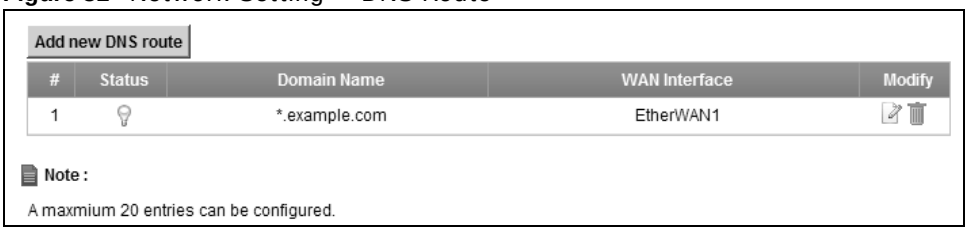
Figure 80 Example of DNS Routing Topology



11.2 The DNS Route Screen

The **DNS Route** screens let you view and configure DNS routes on the Device. Click **Network Setting > DNS Route** to open the **DNS Route** screen.

Figure 81 Network Setting > DNS Route


Add new DNS route
Status Domain Name WAN Interface Modify
1 *.example.com EtherWAN1
Note :
A maxmium 20 entries can be configured.

The following table describes the labels in this screen.

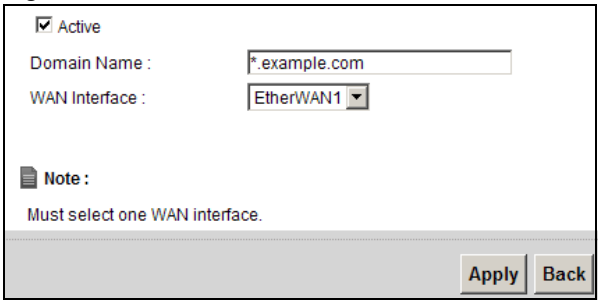
Table 48 Network Setting > DNS Route

LABEL	DESCRIPTION
Add new DNS route	Click this to create a new entry.
#	This is the number of an individual DNS route.
Status	This shows whether the DNS route is currently in use or not. A yellow bulb signifies that this DNS route is in use. A gray bulb signifies that this DNS route is not in use.
Domain Name	This is the domain name to which the DNS route applies.
WAN Interface	This is the WAN interface through which the matched DNS request is routed.
Modify	Click the **Edit** icon to configure a DNS route on the Device. Click the **Delete** icon to remove a DNS route from the Device.

11.2.1 Add/Edit DNS Route Edit

Click **Add new DNS route** in the **DNS Route** screen or the **Edit** icon next to an existing DNS route. Use this screen to configure the required information for a DNS route.

Figure 82 DNS Route: Add/Edit



The following table describes the labels in this screen.

Table 49 DNS Route: Add/Edit

LABEL	DESCRIPTION
Active	Select this to activate this DNS route.
Domain Name	Enter the domain name you want to resolve. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The Device forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
WAN Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interface(s) already configured in the **Broadband** screen.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

12

Interface Group

12.1 Overview

By default, all LAN and WAN interfaces on the Device are in the same group and can communicate with each other. Create interface groups to have the Device assign the IP addresses in different domains to different groups. Each group acts as an independent network on the Device. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

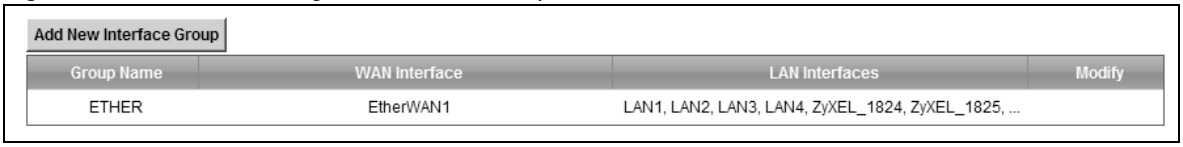
12.2 The Interface Group Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the Device automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the Device assigns to the clients in the default and/or user-defined groups. If you set the Device to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See Chapter 7 on page 121 for more information.

Click **Network Setting > Interface Group** to open the following screen.

Figure 83 Network Setting > Interface Group



The following table describes the fields in this screen.

Table 50 Network Setting > Interface Group

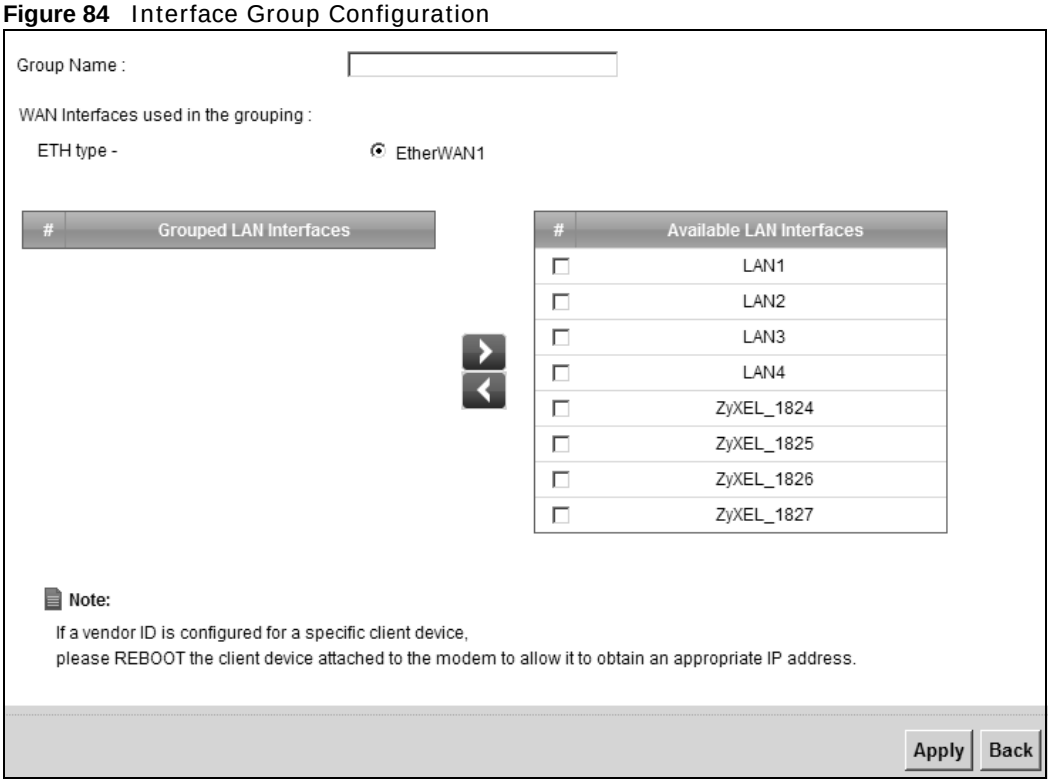
LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Modify	Click the Edit icon to modify the settings. Click the **Delete** icon to remove the group.

12.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Group** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to only one group at a time.

Figure 84 Interface Group Configuration



The following table describes the fields in this screen.

Table 51 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
WAN Interface used in the grouping	Select the WAN interface this group uses.
Grouped LAN Interfaces Available LAN Interfaces	Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the **Available LAN Interfaces** list and use the left arrow to move them to the **Grouped LAN Interfaces** list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the **Grouped LAN Interfaces**, use the right-facing arrow.

13

Firewall

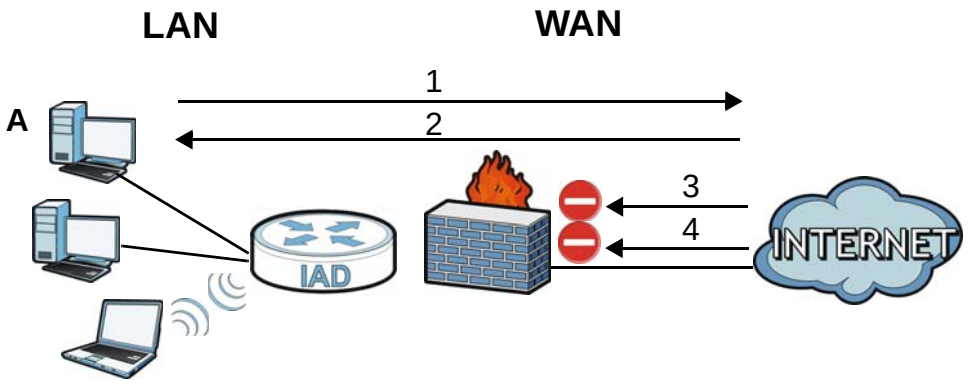
13.1 Overview

Use the Device firewall screens to enable and configure the firewall that protects your Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- Allows traffic that originates from your LAN and WLAN computers to go to all other networks.
- Blocks traffic that originates on other networks from going to the LAN and WLAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (**1**). Return traffic for this session is also allowed (**2**). However other traffic initiated from the WAN is blocked (**3** and **4**).

Figure 85 Default Firewall Action



13.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable the Device's firewall (Section 13.2 on page 178).
- Use the **Services** screen to view the configured firewall rules and add, edit or remove a firewall rule (Section 13.3 on page 179).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 13.4 on page 181).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 13.5 on page 183).

13.1.2 What You Need to Know

Firewall

The Device's firewall feature physically separates the LAN/WLAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is designed to protect against Denial of Service (DoS) attacks when activated. The Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The Device is installed between the LAN/WLAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The Device has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

Finding Out More

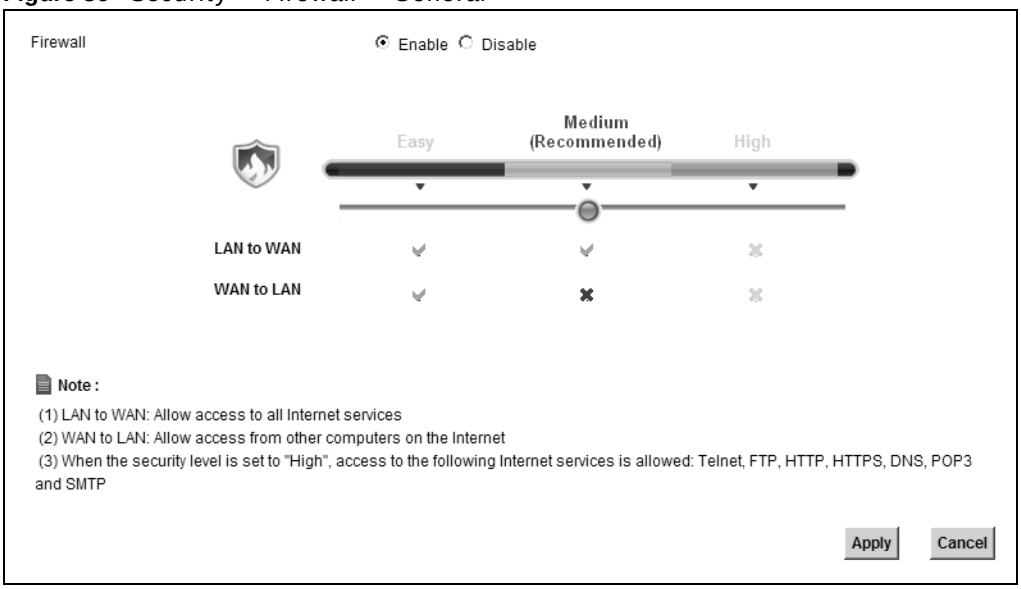
See Section 13.6 on page 183 for advanced technical information on firewall.

13.2 The General Screen

Use this screen to set the security level of the firewall on the Device. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Click **Security > Firewall** to display the **General** screen.

Figure 86 Security > Firewall > General


Firewall
Enable
Disable
Easy
Medium
(Recommended)
High
LAN to WAN
WAN to LAN
Note :
(1) LAN to WAN: Allow access to all Internet services
(2) WAN to LAN: Allow access from other computers on the Internet
(3) When the security level is set to "High", access to the following Internet services is allowed: Telnet, FTP, HTTP, HTTPS, DNS, POP3 and SMTP
Apply
Cancel

The following table describes the labels in this screen.

Table 52 Security > Firewall > General

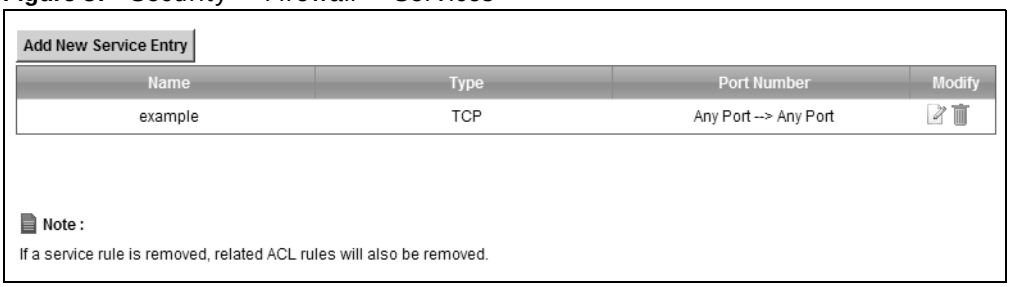
LABEL	DESCRIPTION
Firewall	Select **Enable** to activate the firewall feature on the Device.
Easy	Select **Easy** to allow LAN to WAN and WAN to LAN packet directions.
Medium	Select **Medium** to allow LAN to WAN but deny WAN to LAN packet directions.
High	Select **High** to deny LAN to WAN and WAN to LAN packet directions.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

13.3 The Services Screen

You can configure customized services and port numbers in the **Service** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See Appendix E on page 353 for some examples.

Click **Security > Firewall > Service** to display the following screen.

Figure 87 Security > Firewall > Services



Each field is described in the following table.

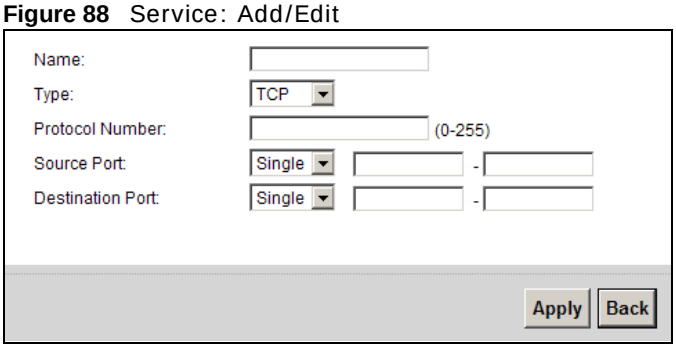
Table 53 Security > Firewall > Services

LABEL	DESCRIPTION
Add New Service Entry	Click this to add a new service.
Name	This is the name of your customized service.
Type	This shows the IP protocol typr.
Port Number	This is the port number or range of ports that defines your customized service.
Modify	Click the **Edit** icon to edit the entry. Click the **Delete** icon to remove this entry.

13.3.1 Add/Edit a Service

Use this screen to add a customized service rule that you can use in the firewall's ACL rule configuration. Click **Add New Service Entry** or the edit icon next to an existing service rule in the **Service** screen to display the following screen.

Figure 88 Service: Add/Edit



The following table describes the labels in this screen.

Table 54 Service: Add/Edit

LABEL	DESCRIPTION
Name	Enter a name for this service.
Type	Choose the IP protocol (**TCP**, **UDP**, **ICMP**, or **Other**) that defines your customized port from the drop-down list box. Select **Other** to be able to enter a protocol number.

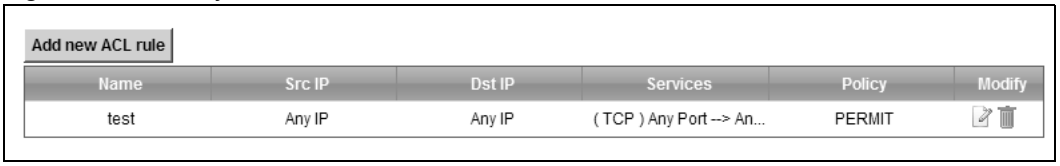
Table 54 Service: Add/Edit (continued)

LABEL	DESCRIPTION
Protocol Number	This field is displayed if you select **Other** as the protocol. Enter the protocol number of your customized port.
Source/ Destination Port	These fields are displayed if you select **TCP** or **UDP** as the IP port. Select **Single** to specify one port only or **Range** to specify a span of ports that define your customized service. If you select **Any**, the service is applied to all ports. Type a single port number or the range of port numbers that define your customized service.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

13.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 89 Security > Firewall > Access Control



The following table describes the labels in this screen.

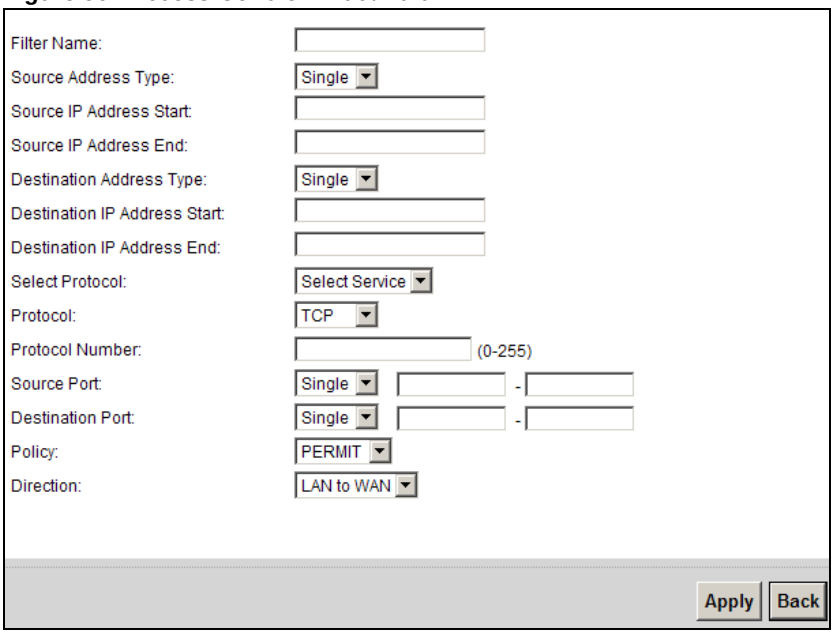
Table 55 Security > Firewall > Access Control

LABEL	DESCRIPTION
Add new ACL rule	Click this to go to add a filter rule for incoming or outgoing IP traffic.
Name	This displays the name of the rule.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to **Any**.
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to **Any**.
Services	This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies.
Policy	This field displays whether the rule silently discards packets (**DROP**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**REJECT**) or allows the passage of packets (**ACCEPT**).
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.

13.4.1 Add/Edit an ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

Figure 90 Access Control: Add/Edit



The following table describes the labels in this screen.

Table 56 Access Control: Add/Edit

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Source Address Type	Select the type of source address.
Source IP Address Start/ End	When the **Source Address Type** field is configured as **Single**, enter the IP address of the source. When the **Source Address Type** field is configured as **Range**, enter the range of source IP address.
Destination Address Type	Select the type of destination address.
Source IP Address Start/ End	When the **Destination Address Type** field is configured as **Single**, enter the IP address of the source. When the **Destination Address Type** field is configured as **Range**, enter the range of source IP address.
Select Protocol	Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the **Security > Firewall > Service > Add** screen display in this list.
Protocol	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Choose the IP port (**TCP**, **UDP**, **ICMP**, or **Others**) that defines your customized port from the drop-down list box.
Protocol Number	If you select **Others** in the **Select Protocol** field, enter a single port number or the range of port numbers of the source.

Table 56 Access Control: Add/Edit (continued)

LABEL	DESCRIPTION
Source/ Destination Port	These fields are displayed if you select **TCP** or **UDP** as the IP port. Select **Single** to specify one port only or **Range** to specify a span of ports that define your customized service. If you select **Any**, the service is applied to all ports. Type a single port number or the range of port numbers that define your customized service.
Policy	Use the drop-down list box to select whether to discard (**DROP**), deny and send an ICMP destination-unreachable message to the sender of (**REJECT**) or allow the passage of (**ACCEPT**) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

13.5 The DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Use the **DoS** screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

Figure 91 Security > Firewall > DoS

The following table describes the labels in this screen.

Table 57 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Select **Enable** to enable protection against DoS attacks.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

13.6 Firewall Technical Reference

This section provides some technical background information about the topics covered in this chapter.

13.6.1 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your Device.
4. Don't enable any local service (such as Telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Keep the firewall in a secured (locked) room.

13.6.2 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

   Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

14

MAC Filter

14.1 Overview

This chapter discusses MAC address filtering.

You can configure the Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections.

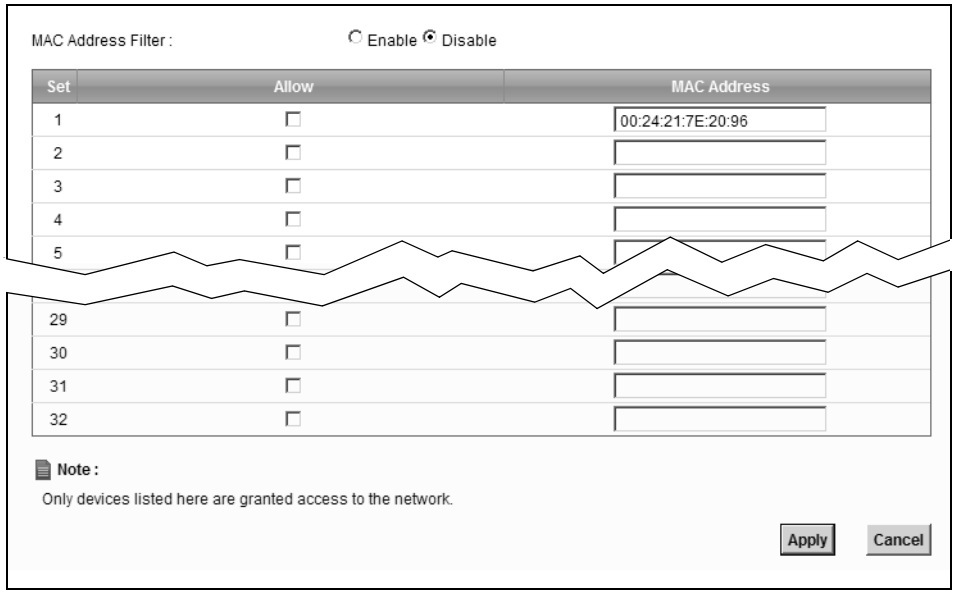
14.1.1 What You Need to Know

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

14.2 The MAC Filter Screen

Use the **MAC Filter** screen to allow wireless and LAN clients access to the Device. To change your Device's MAC filter settings, click **Security** > **MAC Filter**. The screen appears as shown.

Figure 92 Security > MAC Filter



The following table describes the labels in this menu.

Table 58 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select **Enable** to activate MAC address filtering.
Set	This is the index number of the MAC address.
Allow	Select **Allow** to permit access to the Device. MAC addresses not listed will be denied access to the Device. If you clear this, the **MAC Address** field for this set clears.
MAC Address	Enter the MAC addresses of the wireless station and LAN devices that are allowed access to the Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

15

Parental Control

15.1 Overview

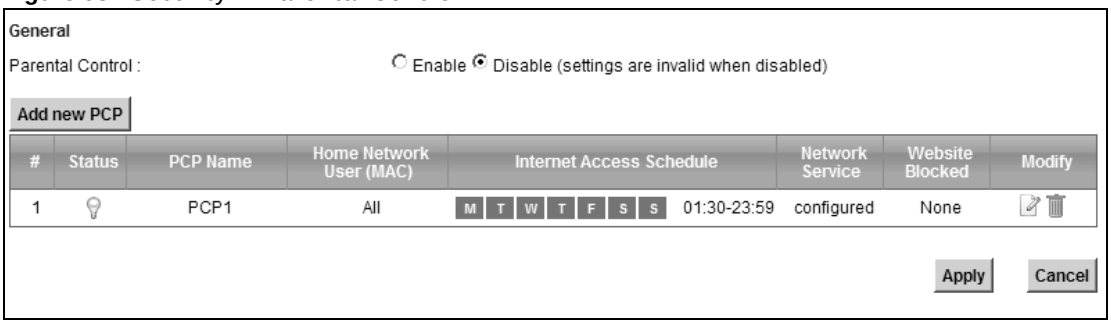
Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the Device performs parental control on a specific user.

15.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Security > Parental Control** to open the following screen.

Figure 93 Security > Parental Control


General
Parental Control :
Enable
Disable (settings are invalid when disabled)
Add new PCP
Status PCP Name Home Network User (MAC) Internet Access Schedule Network Service Website Blocked Modify
1 PCP1 All M T W T F S S 01:30-23:59 configured None
Apply
Cancel

The following table describes the fields in this screen.

Table 59 Parental Control > Parental Control

LABEL	DESCRIPTION
Parental Control	Select **Enable** to activate parental control.
Add new PCP	Click this if you want to configure a new parental control rule.
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User (MAC)	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.

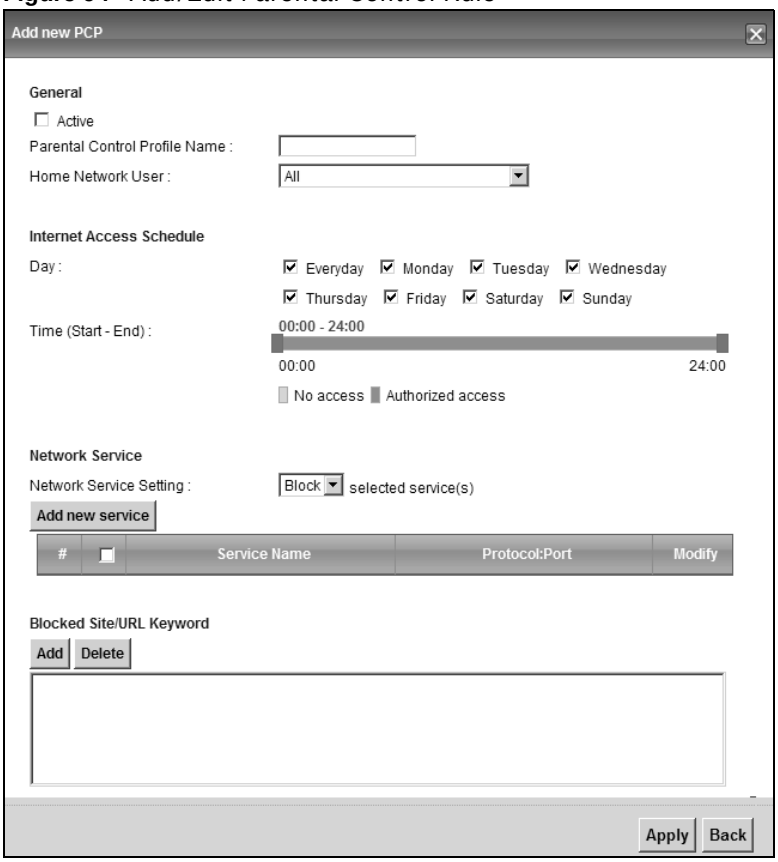
Table 59 Parental Control > Parental Control (continued)

LABEL	DESCRIPTION
Network Service	This shows whether the network service is configured. If not, **None** will be shown.
Website Block	This shows whether the website block is configured. If not, **None** will be shown.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Add	Click **Add** to create a new schedule.
Apply	Click **Apply** to save your changes back to the Device.

15.2.1 Add/Edit a Parental Control Rule

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 94 Add/Edit Parental Control Rule



The following table describes the fields in this screen.

Table 60 Add/Edit Parental Control Rule

LABEL	DESCRIPTION
General	
Active	Select the checkbox to activate this parental control rule.

Table 60 Add/Edit Parental Control Rule (continued)

LABEL	DESCRIPTION
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select **Custom**, enter the LAN user's MAC address. If you select **All**, the rule applies to all LAN users.
Internet Access Schedule	
Day	Select check boxes for the days that you want the Device to perform parental control.
Time	Drag the time bar to define the time that the LAN user is allowed access.
Network Service	
Network Service Setting	If you select **Block**, the Device prohibits the users from viewing the Web sites with the URLs listed below. If you select **Access**, the Device blocks access to all URLs except ones listed below.
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the **Service Name**, **Protocol**, and **Name** of the new rule.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Blocked Site/ URL Keyword	Click **Add** to show a screen to enter the URL of web site or URL keyword to which the Device blocks access. Click **Delete** to remove it.
Apply	Click this button to save your settings back to the Device.
Back	Click this button to return to the previous screen without saving any changes.

16

Certificates

16.1 Overview

The Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

16.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Device's CA-signed certificates (Section 16.2 on page 193).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Device. You can also export the certificates to a computer (Section 16.3 on page 195).
- Use the **VPN Certificates** screen to view and import the Device's VPN certificates (Section 16.6 on page 197).

16.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Certification Path

A certification path is the hierarchy of certification authority certificates that validate a certificate. The Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certificate Directory Servers

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

16.1.3 Verifying a Certificate

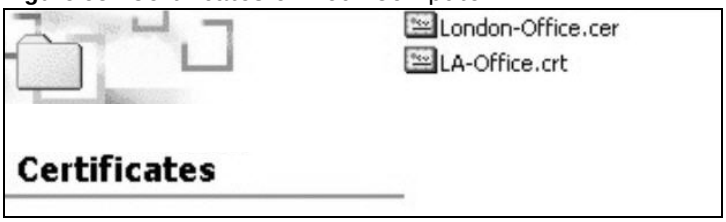
Before you import a trusted CA or trusted remote host certificate into the Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

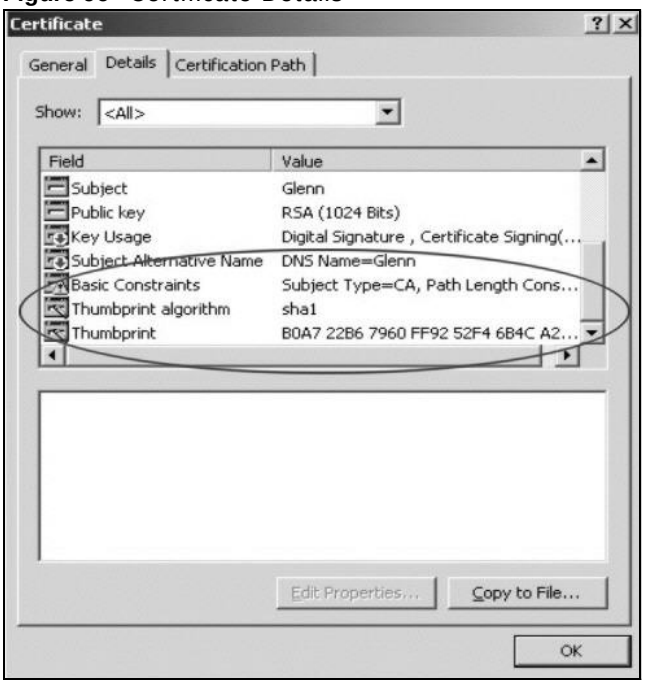
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 95 Certificates on Your Computer



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 96 Certificate Details



4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

16.2 Local Certificates

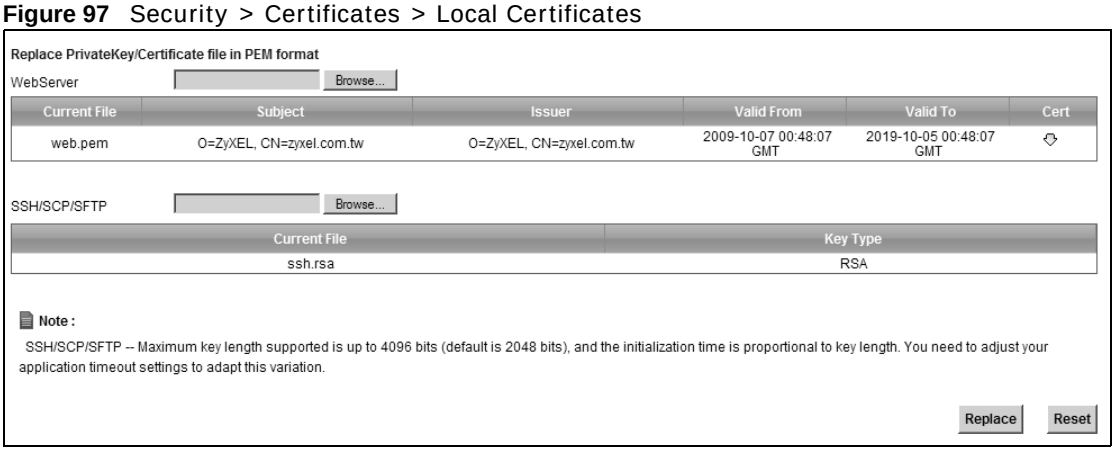
Use this screen to view the Device's summary list of certificates and certification requests. You can import the following certificates to your Device:

- Web Server - This certificate secures HTTP connections.

- SIP TLS - This certificate secures VoIP connections.
- SSH/SCP/SFTP - This certificate secures remote connections.

Click **Security > Certificates** to open the **Local Certificates** screen.

Figure 97 Security > Certificates > Local Certificates



The following table describes the labels in this screen.

Table 61 Security > Certificates > Local Certificates

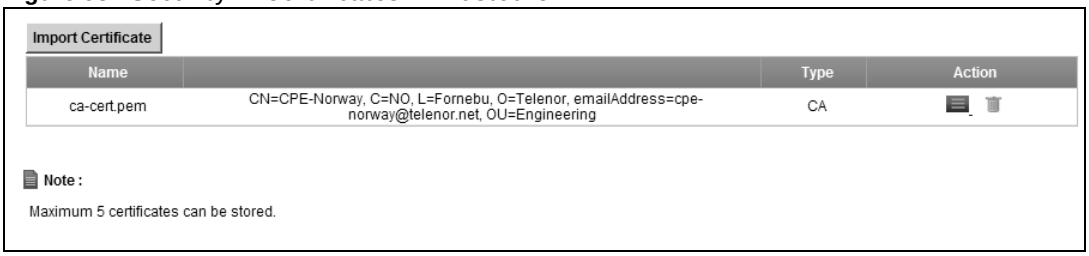
LABEL	DESCRIPTION
WebServer	Click **Browse...** to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Cert	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
SSH/SCP/SFTP	Type in the location of the **SSH / SCP / SFTP** certificate file you want to upload in this field or click **Browse** to find it.
Choose file	Click this link to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Key Type	This field applies to the **SSH / SCP / SFTP** certificate. This shows the file format of the current certificate.
Replace	Click this to replace the certificate(s) and save your changes back to the Device.
Reset	Click this to clear your settings.

16.3 Trusted CA

Use this screen to view a summary list of certificates of the certification authorities that you have set the Device to accept as trusted. The Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Click **Security > Certificates > Trusted CA** to open the **Trusted CA** screen.

Figure 98 Security > Certificates > Trusted CA



The following table describes the labels in this screen.

Table 62 Security > Certificates > Trusted CA

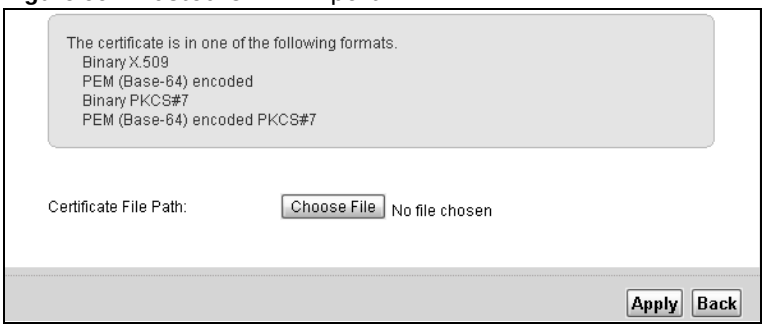
LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Device.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Action	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Delete** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

16.4 Trusted CA Import

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. You can save a trusted certification authority's certificate to the Device.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 99 Trusted CA > Import



The following table describes the labels in this screen.

Table 63 Security > Certificates > Trusted CA > Import

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the Device.
Back	Click **Back** to return to the previous screen.

16.5 View Certificate

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Click **Security** > **Certificates** > **Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 100 Trusted CA: View

The following table describes the labels in this screen.

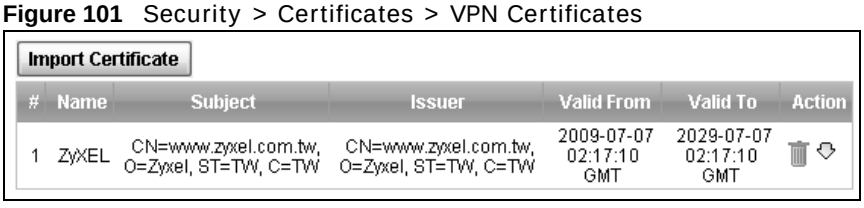
Table 64 Trusted CA: View

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certificate Detail	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this to return to the previous screen.

16.6 VPN Certificates

To access this screen, click on **Security** > **Certificates** > **VPN Certificates**.

Figure 101 Security > Certificates > VPN Certificates


Import Certificate
Name Subject Issuer Valid From Valid To Action
1 ZyXEL CN=www.zyxel.com.tw, O=Zyxel, ST=TW, C=TW CN=www.zyxel.com.tw, O=Zyxel, ST=TW, C=TW 2009-07-07 02:17:10 GMT 2029-07-07 02:17:10 GMT

The following table describes the labels in this screen.

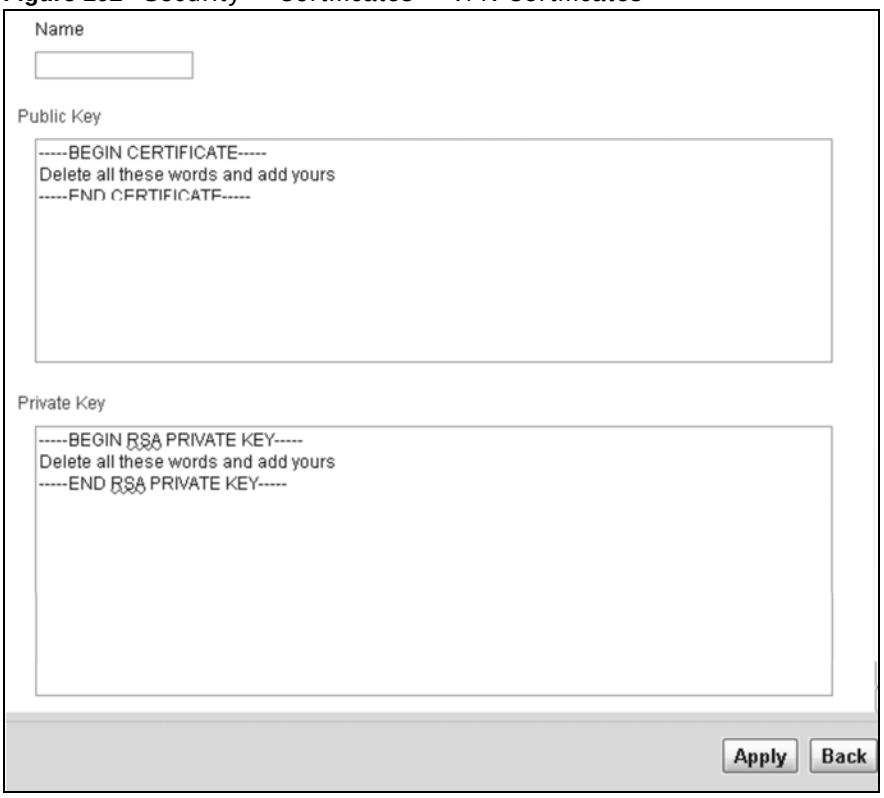
Table 65 Security > Certificates > VPN Certificates

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Device.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Action	Click the **Delete** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.). Click on the **Download** icon to download a certificate to your computer.

16.6.1 Import Certificate

Click **Import Certificate** in the **VPN Certificates** screen to open the **Import Certificate** screen. You can save a trusted certification authority's certificate to the Device.

Figure 102 Security > Certificates > VPN Certificates



The following table describes the labels in this screen.

Table 66 VPN Certificates > Import

LABEL	DESCRIPTION
Name	Type a name for this certificate
Public Key	The value provided by a designated authority, which combined with a private key, can be used to encrypt messages. Write the key between **BEGIN CERTIFICATE** and **END CERTIFICATE**.
Private Key	This is the key known only to the parties that exchange information. Write the key between **BEGIN CERTIFICATE** and **END CERTIFICATE**.
Apply	Click **Apply** to save the certificate on the Device.
Back	Click **Back** to return to the previous screen.

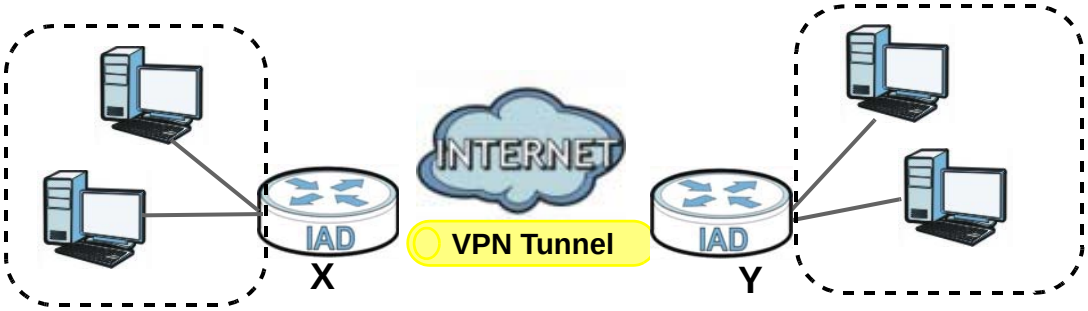
17 VPN

17.1 Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The following figure is an example of an IPSec VPN tunnel.

Figure 103 VPN: Example



17.1.1 What You Can Do in the VPN Screens

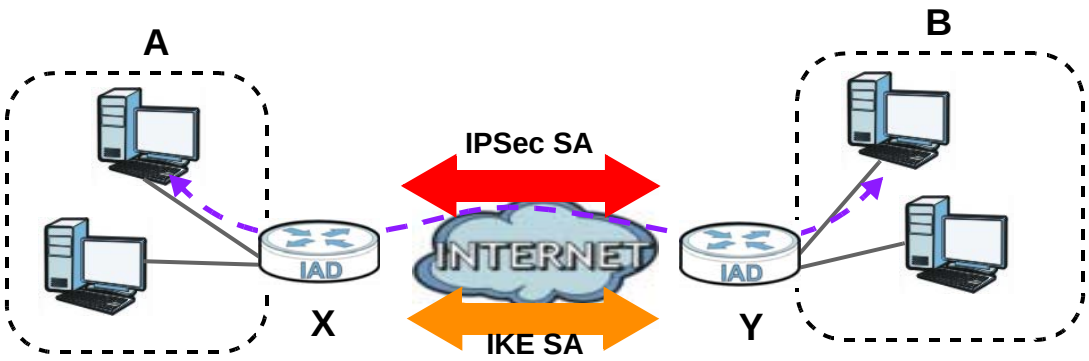
- Use the **Setup** screen (Section 17.2 on page 203) to view the configured VPN policies and add, edit or remove a VPN policy.
- Use the **Monitor** screen (Section 17.5 on page 210) to display and manage the current active VPN connections.

17.1.2 What You Need to Know About IPSec VPN

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the Device and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the Device and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which

the Device and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 104 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

My IP Address

My IP Address is the WAN IP address of the Device. The Device has to rebuild the VPN tunnel if **My IP Address** changes after setup.

The following applies if this field is configured as **0.0.0.0**:

- The Device uses the current Device WAN IP address (static or dynamic) to set up the VPN tunnel.

Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The Device has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

Dynamic Secure Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network (see Section 17.6.11 on page 217 for configuration examples).

The Secure Gateway IP Address may be configured as **0.0.0.0** only when using **IKE** key management and not **Manual** key management.

Finding Out More

See Section 17.6 on page 210 for advanced technical information on IPSec VPN.

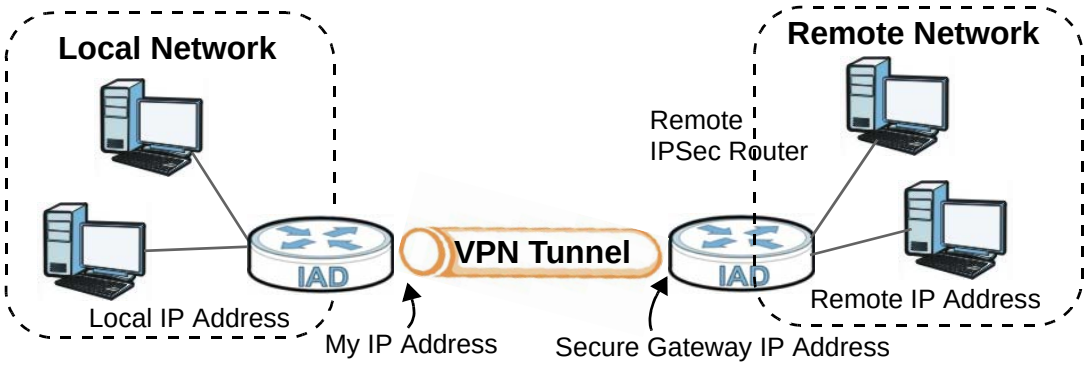
17.1.3 Before You Begin

If a VPN tunnel uses Telnet, FTP, WWW, then you should configure remote management (**Remote MGMT**) to allow access for that service.

17.2 VPN Setup Screen

The following figure helps explain the main fields in the web configurator.

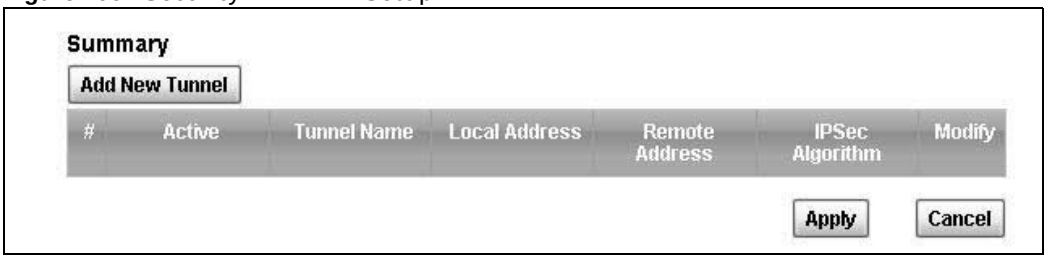
Figure 105 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **Security** > **VPN** to open the **VPN Setup** screen. This is a menu of your IPSec rules (tunnels). The IPSec summary menu is read-only. Edit a VPN by selecting an index number and then configuring its associated submenus.

Figure 106 Security > VPN > Setup



The following table describes the fields in this screen.

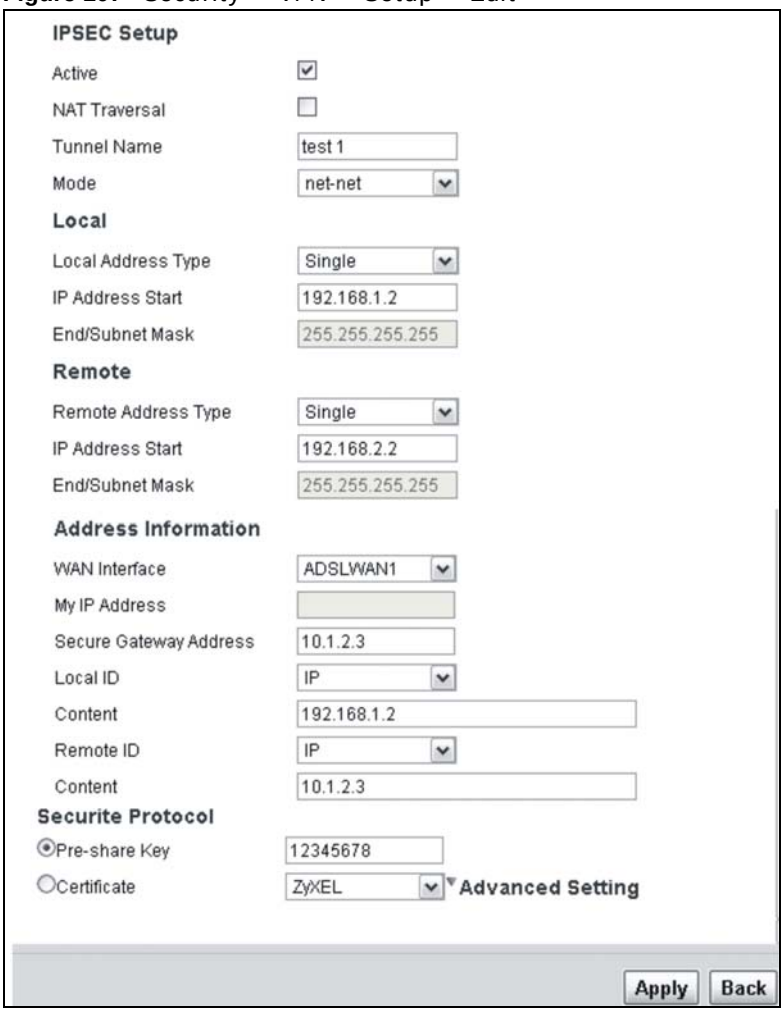
Table 67 Security > VPN > Setup

LABEL	DESCRIPTION
Add New Tunnel	Click this button to set up VPN policies for a new tunnel
#	This is the VPN policy index number. Click a number to edit VPN policies.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.
Tunnel Name	This field displays the identification name for this VPN policy.
Local Address	This field will display the IP address used by the Device.
Remote Address	This field will display the Secure Gateway Address of the IPSec router with which you're making the VPN connection
IPSec Algorithm	This field displays the encryption algorithm used for an SA. Both **AH** and **ESP** increase Device processing requirements and communications latency (delay).
Modify	Click the **Edit** icon to go to the screen where you can edit the VPN configuration. Click the **Remove** icon to remove an existing VPN configuration.
Apply	Click this to save your changes and apply them to the Device.
Cancel	Click this return your settings to their last saved values.

17.3 The VPN Edit Screen

Click on **Add New Tunnel** in the **VPN Setup** screen or click on the **Edit** icon to edit VPN policies. Both commands share the same screen.

Figure 107 Security > VPN > Setup > Edit



The following table describes the fields in this screen.

Table 68 Security > VPN > Setup > Edit

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
NAT Traversal	Select this check box if you want to set up a VPN tunnel when there are NAT routers between the Device and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 4500 packets to the remote IPSec router behind the NAT router.
Tunnel Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the Device drops trailing spaces.
Mode	Select **net-net** or **Roadwarrior** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

Table 68 Security > VPN > Setup > Edit (continued)

LABEL	DESCRIPTION
Local	Specify the IP addresses of the devices behind the Device that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose **Single**, or **Subnet**. Select **Single** for a single IP address. Select **Subnet** to specify IP addresses based on the subnet mask.
IP Address Start	When the **Local Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your Device. When the **Local Address Type** field is configured to **Subnet**, enter an IP address on the LAN behind your Device.
End / Subnet Mask	When the **Local Address Type** field is configured to **Single**, this field is N/A. When the **Local Address Type** field is configured to **Subnet**, enter the subnet of the LAN behind your Device.
Remote	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose **Single**, or **Subnet**. Select **Single** for a single IP address. Select **Subnet** to specify IP addresses based on the subnet mask.
IP Address Start	When the **Remote Address Type** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter an IP Address on the LAN behind the IPSec router.
End / Subnet Mask	When the **Remote Address Type** field is configured to **Single**, this field is N/A. When the **Remote Address Type** field is configured to **Subnet**, enter the subnet of the LAN behind the IPSec router.
Address Information	
WAN Interface	The interface used to connect to the internet
My IP Address	My IP Address only shows the IP of the selected interface. There is no need to modify this information.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. If you are not sure of this information you can leave it blank, but do not use 0.0.0.0.
Local ID	Select **IP** to identify this Device by its IP address. Select **DNS** to identify this Device by a domain name. Select **E-mail** to identify this Device by an e-mail address.

Table 68 Security > VPN > Setup > Edit (continued)

LABEL	DESCRIPTION
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The Device automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this Device in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Remote ID	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the Device will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
Security Protocol	
Pre-Shared Key	Click the button to use a pre-shared key for authentication, and type in your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
Certificate	Click the button to use a certificate for authentication. Select the certificate you want to use from the list. You can create, import and configure certificates in the **Security > Certificates** screens.

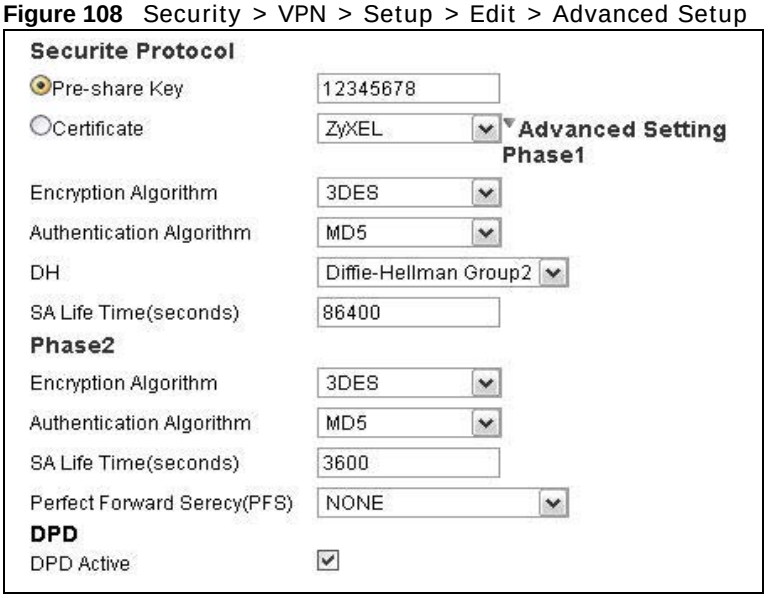
Table 68 Security > VPN > Setup > Edit (continued)

LABEL	DESCRIPTION
Advanced Setup	Click **Advanced Setup** to configure more detailed settings of your IKE key management.
Apply	Click **Apply** to save your changes back to the Device.
Back	Click **Back** to return to the previous screen.

17.4 Configuring Advanced Settings

Click **Advanced Setup** in the **VPN Setup-Edit** screen to open this screen.

Figure 108 Security > VPN > Setup > Edit > Advanced Setup



The following table describes the fields in this screen.

Table 69 Security > VPN > Setup > Edit > Advanced Setup

LABEL	DESCRIPTION
Phase 1	
Encryption Algorithm	Select **3DES**, **AES128** or **AES256** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key and a 256-bit key. **AES** is faster than **3DES**.

Table 69 Security > VPN > Setup > Edit > Advanced Setup (continued)

LABEL	DESCRIPTION
Authentication Algorithm	Select **MD5**, **SHA1**, **SHA2-256** or **SHA2-512** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) and **SHA2** are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for more security. **SHA2-256** or **SHA2-512** are part of the SHA2 set of cryptographic functions and they are considered even more secure than **MD5** and **SHA1**.
DH	You must choose a key group for phase 1 setup. **DH2** refers to Diffie-Hellman Group 2, a 1024-bit random number. **DH5** refers to Diffie-Hellman Group5, a 1536-bit random number, and **DH14** refers to Diffie-Hellman Group 14, providing 2048 bits of key strength.
SA Life Time (Seconds)	Define the length of time before an IPSec SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Phase 2	
Encryption Algorithm	Select **3DES, AES-128** or **AES-256** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a **128**-bit key and a **256**-bit key. **AES** is faster than **3DES**.
Authentication Algorithm	Select **MD5**, **SHA1**, **SHA2-256** or **SHA2-512** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) and **SHA2** are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for more security. **SHA2-256** or **SHA2-512** are part of the SHA2 set of cryptographic functions and they are considered even more secure than **MD5** and **SHA1**.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose **DH2**, **DH5** or **DH14** from the drop-down list box to enable PFS. **DH2** refers to Diffie-Hellman Group 2, a 1024-bit random number. **DH5** refers to Diffie-Hellman Group5, a 1536-bit random number, and **DH14** refers to Diffie-Hellman Group 14, providing 2048 bits of key strength.
DPD Active	Select DPD (Dead Peer Protection) if you want the Device to make sure the remote IPSec router is there before it transmits data. The remote IPSec router must support DPD. If there has been no traffic for at least 15 seconds, the Device sends a message to the remote IPSec router. If the remote IPSec router responds, the Device transmits the data. If the remote IPSec router does not respond, the Device shuts down the SA.
Apply	Click **Apply** to save your changes back to the Device and return to the **VPN** screen.
Back	Click **Back** to return to the previous screen.

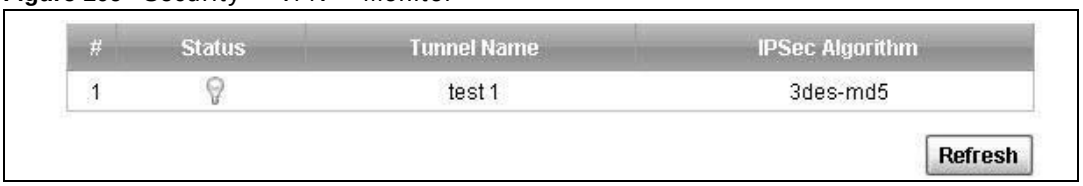
17.5 Viewing SA Monitor

Click **Security** > **VPN** > **Monitor** to open the screen as shown. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See Section 17.6.6 on page 215 on keeping alive to have the Device renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 109 Security > VPN > Monitor



The following table describes the fields in this screen.

Table 70 Security > VPN > Monitor

LABEL	DESCRIPTION
No	This is the security association index number.
Status	Displays whether the security association is active or not
Tunnel Name	This is the name of the new tunnel.
IPSec Algorithm	This field displays the encryption algorithm, and authentication algorithm used in each VPN tunnel.
Disconnect	Select one of the security associations, and then click **Disconnect** to stop that security association.
Refresh	Click **Refresh** to display the current active VPN connection(s).

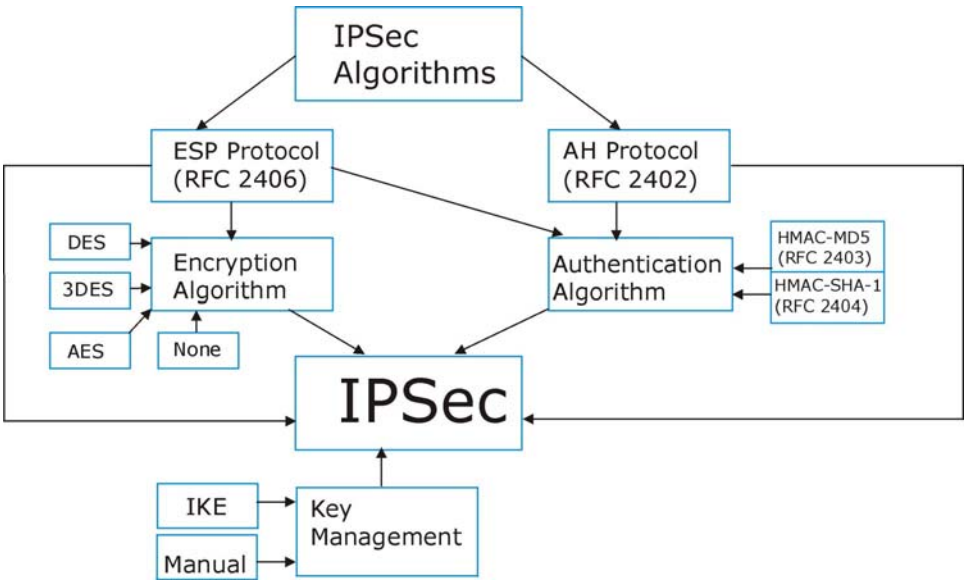
17.6 IPSec VPN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

17.6.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 110 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

17.6.2 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the

incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 71 VPN and NAT

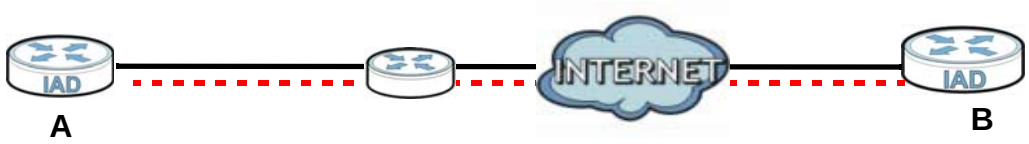
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

17.6.3 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the Device's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 111 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In Figure 111 on page 212, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 72 VPN and NAT

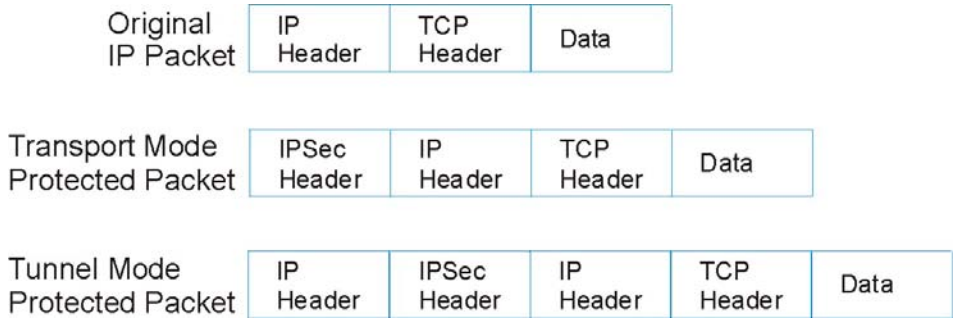
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the Device if you enable NAT traversal.

17.6.4 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 112 Transport and Tunnel Mode IPSec Encapsulation



Tunnel Mode

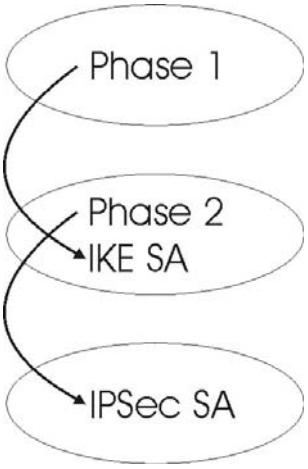
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

17.6.5 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 113 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see Appendix D on page 333. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The Device also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

17.6.6 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

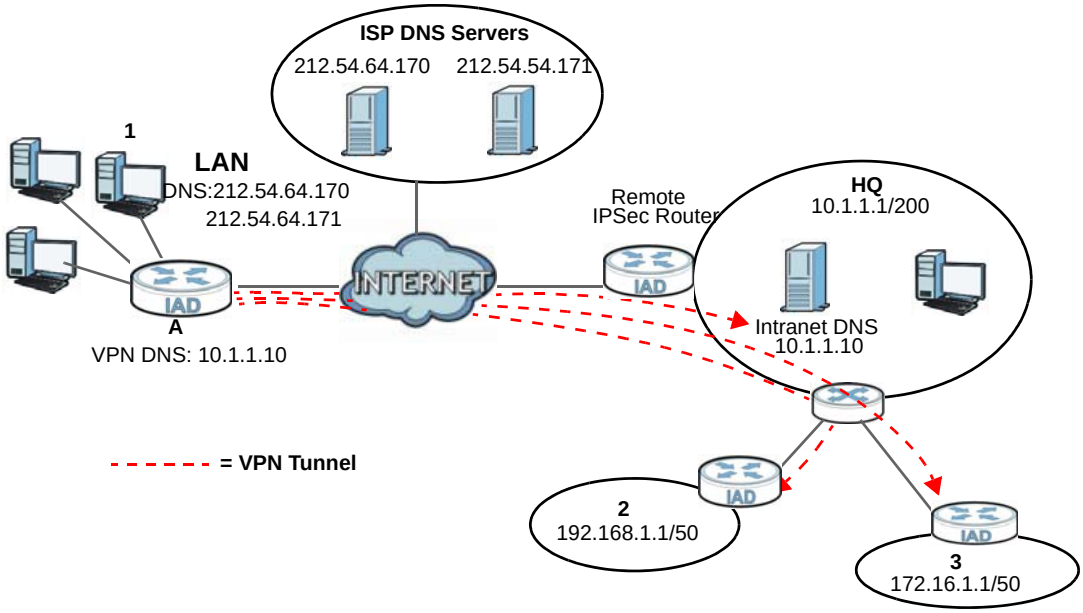
- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).

17.6.7 Remote DNS Server

In cases where you want to use domain names to access Intranet servers on a remote network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote network

The following figure depicts an example where three VPN tunnels are created from Device A; one to branch office 2, one to branch office 3 and another to headquarters. In order to access computers that use private domain names on the headquarters (HQ) network, the Device at branch office 1 uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP.

Figure 114 VPN Host using Intranet DNS Server Example



If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote network.

17.6.8 ID Type and Content

With aggressive negotiation mode (seeSection 17.6.6 on page 215), the Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the Device from IPSec routers with dynamic IP addresses (seeSection 17.6.11 on page 217 for a telecommuter configuration example).

Regardless of the ID type and content configuration, the Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (seeSection 17.6.6 on page 215), the ID type and content are encrypted to provide identity protection. In this case the Device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The Device can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (seeSection 17.4 on page 208). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 73 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the Device automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this Device.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this Device.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

Table 74 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Device automatically use the address in the **Secure Gateway Address** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field below.

17.6.8.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two Devices in this example can complete negotiation and establish a VPN tunnel.

Table 75 Matching ID Type and Content Configuration Example

DEVICE A	DEVICE B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two Devices in this example cannot complete their negotiation because Device B's **Local ID type** is **IP**, but Device A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 76 Mismatching ID Type and Content Configuration Example

DEVICE A	DEVICE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

17.6.9 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 17.6.5 on page 214 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

17.6.10 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

17.6.11 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single Device at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The Device at headquarters has a static public IP address.

17.6.11.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a Device at headquarters (**HQ** in the figure). The telecommuters do not have domain names mapped to the WAN IP

addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

Figure 115 Telecommuters Sharing One VPN Rule Example

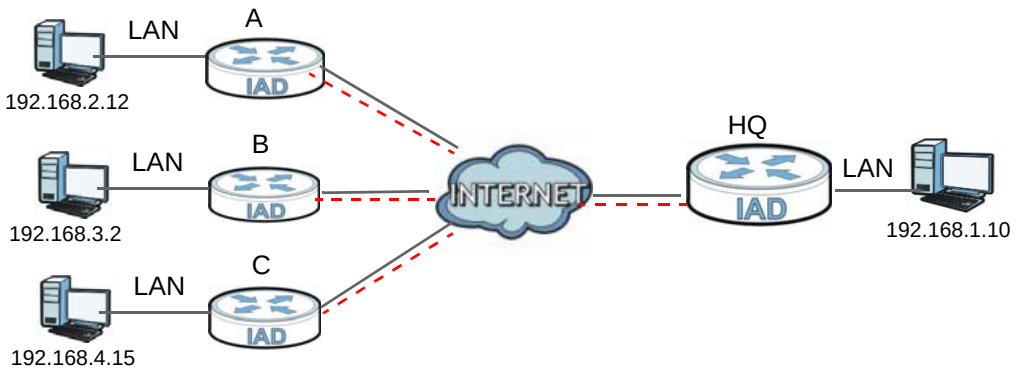


Table 77 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.
Local IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote IP Address:	192.168.1.10	0.0.0.0 (N/A)

17.6.11.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (**A**, **B** and **C** in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see Section 17.6.6 on page 215), the Device can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a Device at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the Device at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a Device located at headquarters. The Device at headquarters (**HQ** in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The Device at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

Figure 116 Telecommuters Using Unique VPN Rules Example

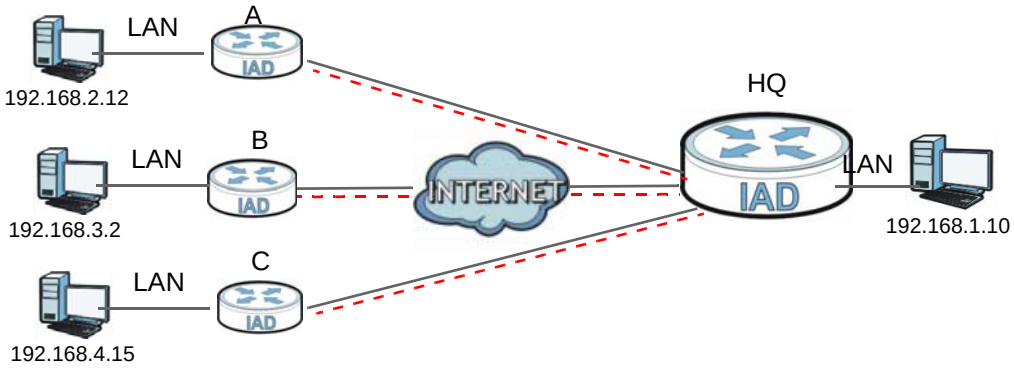


Table 78 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Telecommuter A (telecommutera.dydns.org)	Headquarters Device Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Secure Gateway Address: telecommuter1.com
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters Device Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters Device Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

18 VoIP

18.1 Overview

Use this chapter to:

- Connect an analog phone to the Device.
- Make phone calls over the Internet, as well as the regular phone network.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

18.1.1 What You Can Do in this Chapter

These screens allow you to configure your Device to make phone calls over the Internet and your regular phone line, and to set up the phones you connect to the Device.

- Use the **SIP Service Provider** screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions (Section 18.3 on page 226).
- Use the **SIP Account** screen to set up information about your SIP account, control which SIP accounts the phones connected to the Device use and configure audio settings such as volume levels for the phones connected to the ZyXEL Device (Section 18.3 on page 226).
- Use the **Phone Device** screen to control which SIP accounts the phones connected to the Device use (Section 18.5 on page 230).
- Use the **Region** screen to change settings that depend on the country you are in (Section 18.6 on page 231).
- Use the **Call Rule** screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers (Section 18.7 on page 232).

You don't necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

18.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

SIP stands for Session Initiation Protocol. SIP is a signalling standard that lets one network device (like a computer or the Device) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your Device, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call.

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the Device to use your SIP account to make calls, the Device is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you don't need a SIP account. It is possible for one SIP device (like the Device) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup - figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the Device reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

Comfort Noise Generation

When using VAD, the Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

Use this screen to maintain basic information about each SIP account. You can also enable and disable each SIP account, configure the volume, echo cancellation and VAD (Voice Activity Detection) settings for each individual phone port on the Device.

How to Find Out More

See Chapter 3 on page 31 for a tutorial showing how to set up these screens in an example scenario.

See Section on page 232 for advanced technical information on SIP.

18.1.3 Before You Begin

- Before you can use these screens, you need to have a VoIP account already set up. If you don't have one yet, you can sign up with a VoIP service provider over the Internet.

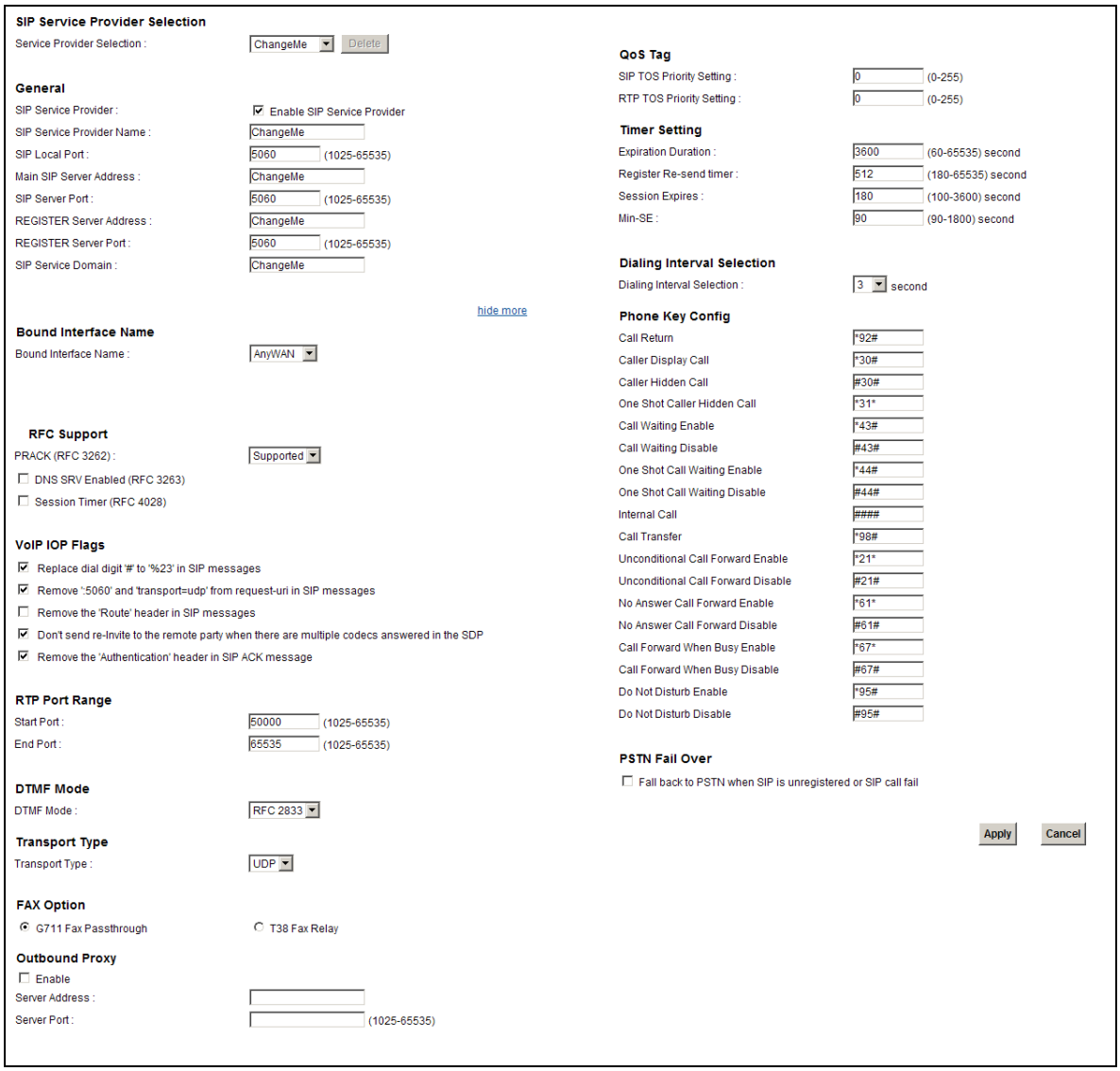
- You should have the information your VoIP service provider gave you ready, before you start to configure the Device.

18.2 The SIP Service Provider Screen

Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions and dialing plan. Click **VoIP > SIP** to open the **SIP Service Provider** screen.

Note: Click **more...** to see all the fields in the screen. You don't necessarily need to use all these fields to set up your account. Click **hide more** to see and configure only the fields needed for this feature.

Figure 117 VoIP > SIP > SIP Service Provider


SIP Service Provider Selection
Service Provider Selection : ChangeMe Delete
General
SIP Service Provider : Enable SIP Service Provider
SIP Service Provider Name : ChangeMe
SIP Local Port : 5060 (1025-65535)
Main SIP Server Address : ChangeMe
SIP Server Port : 5060 (1025-65535)
REGISTER Server Address : ChangeMe
REGISTER Server Port : 5060 (1025-65535)
SIP Service Domain : ChangeMe
hide more
Bound Interface Name
Bound Interface Name : AnyWAN
RFC Support
PRACK (RFC 3262) : Supported
DNS SRV Enabled (RFC 3263)
Session Timer (RFC 4028)
VoIP IOP Flags
Replace dial digit '#' to '%23' in SIP messages
Remove ':5060' and 'transport=udp' from request-uri in SIP messages
Remove the 'Route' header in SIP messages
Don't send re-Invite to the remote party when there are multiple codecs answered in the SDP
Remove the 'Authentication' header in SIP ACK message
RTP Port Range
Start Port : 50000 (1025-65535)
End Port : 65535 (1025-65535)
DTMF Mode
DTMF Mode : RFC 2833
Transport Type
Transport Type : UDP
FAX Option
G711 Fax Passthrough
T38 Fax Relay
Outbound Proxy
Enable
Server Address :
Server Port : (1025-65535)
QoS Tag
SIP TOS Priority Setting : 0 (0-255)
RTP TOS Priority Setting : 0 (0-255)
Timer Setting
Expiration Duration : 3600 (60-65535) second
Register Re-send timer : 512 (180-65535) second
Session Expires : 180 (100-3600) second
Min-SE : 90 (90-1800) second
Dialing Interval Selection
Dialing Interval Selection : 3 second
Phone Key Config
Call Return *92#
Caller Display Call *30#
Caller Hidden Call #30#
One Shot Caller Hidden Call *31*
Call Waiting Enable *43#
Call Waiting Disable #43#
One Shot Call Waiting Enable *44#
One Shot Call Waiting Disable #44#
Internal Call ####
Call Transfer *98#
Unconditional Call Forward Enable *21*
Unconditional Call Forward Disable #21#
No Answer Call Forward Enable *61*
No Answer Call Forward Disable #61#
Call Forward When Busy Enable *67*
Call Forward When Busy Disable #67#
Do Not Disturb Enable *95#
Do Not Disturb Disable #95#
PSTN Fail Over
Fall back to PSTN when SIP is unregistered or SIP call fail
Apply
Cancel

The following table describes the labels in this screen.

Table 79 VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
SIP Service Provider Selection	
Service Provider Selection	Select the SIP service provider profile you want to use for the SIP account you configure in this screen. If you change this field, the screen automatically refreshes.
General	
SIP Service Provider	Select this if you want the Device to use this SIP provider. Clear it if you do not want the Device to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
Bound Interface Name	
Bound Interface Name	If you select **AnyWAN**, the Device automatically activates the VoIP service when any LAN or WAN connection is up.
RFC Support	
PRACK	PRACK (RFC 3262) defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select **Supported** or **Required** to have the Device include a SIP Require/ Supported header field with the option tag 100rel in all INVITE requests. When the Device receives a SIP response message indicating that the phone it called is ringing, the Device sends a PRACK message to have both sides confirm the message is received. If you select **Supported**, the peer device supports the option tag 100rel to send provisional responses reliably. If you select **Required**, the peer device requires the option tag 100rel to send provisional responses reliably. Select **Disabled** to turn off this function.
DNS SRV Enabled	Select this to have the Device query your ISP's DNS server for a list of any available SIP servers that it maintains. This is useful if your static SIP server exeriences difficulties, making it hard for your IP phone users to make SIP calls.
Session Timer	Select this to have the Device support RFC 4028. This makes sure that SIP sessions do not hang and the SIP line can always be available for use.
VoIP IOP Flags	Select the VoIP inter-operability settings you want to activate.

Table 79 VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.
DTMF Mode	Control how the Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC2833** - send the DTMF tones in RTP packets. **PCM** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. **SIP INFO** - send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the transport layer protocol **UDP** or **TCP** (usually UDP) used for SIP.
FAX Option	This field controls how the Device handles fax messages.
G711 Fax Passthrough	Select this if the Device should use G.711 to send fax messages. The peer devices must also use G.711.
T38 Fax Relay	Select this if the Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
Outbound Proxy	
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
QoS Tag	
SIP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the Device accepts.

Table 79 VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
Phone Key Config	Specify the key combinations for certain functions of the SIP phone.
PSTN Fail Over	Select this check box if you want to redirect the outgoing calls to the PSTN line (that do not use the Internet) when your SIP account is unregistered or SIP call has failed.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

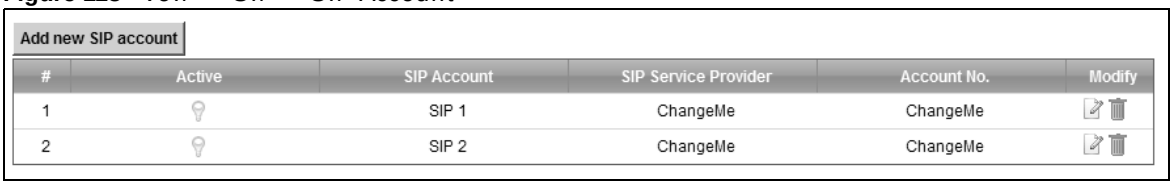
18.3 The SIP Account Screen

The Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your Device to connect to your VoIP service provider.

See Section 18.3 on page 226 for how to map a SIP account to a phone port.

To access the following screen, click **VoIP > SIP > SIP Account**.

Figure 118 VoIP > SIP > SIP Account



The following table describes the labels in this screen.

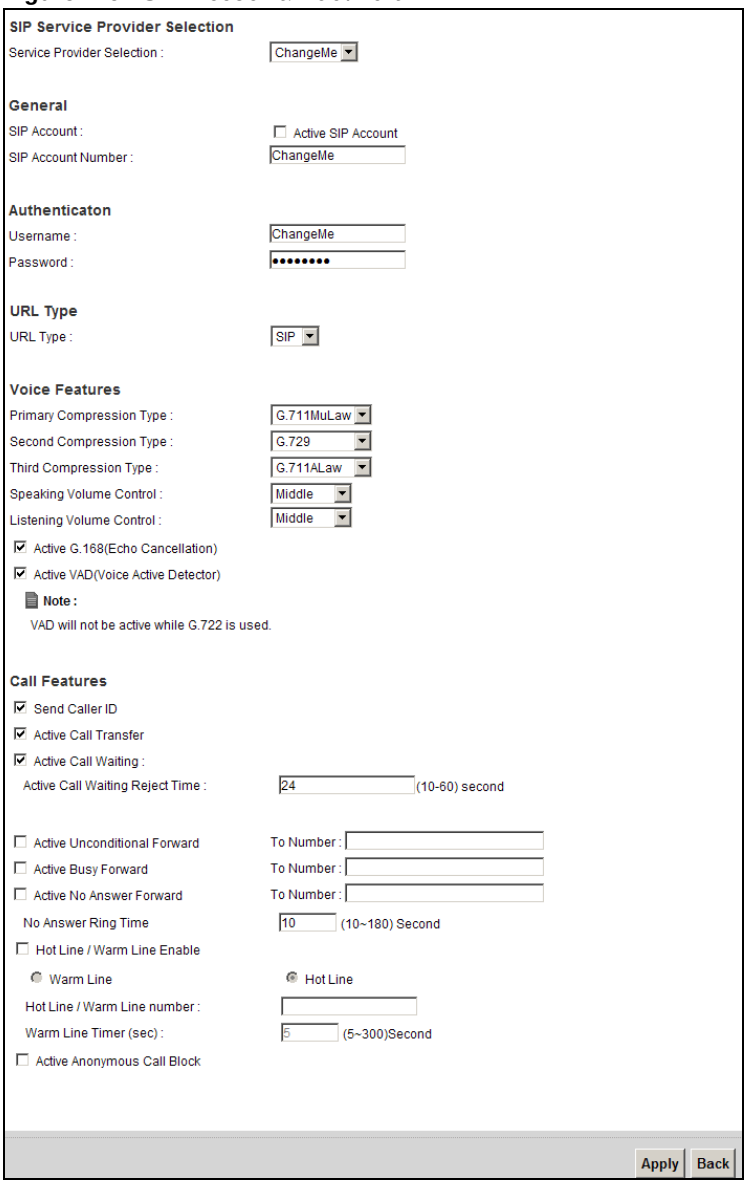
Table 80 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
#	This is the index number of the entry.
Active	This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is activated.
SIP Account	This shows the name of the SIP account.
SIP Service Provider	This shows the name of the SIP service provider.
Account No.	This shows the SIP number.
Modify	Click the **Edit** icon to configure the SIP account. Click the **Delete** icon to delete this SIP account from the Device.

18.3.1 Add/Edit SIP Account

You can configure a new SIP account or edit one. To access this screen, click **Add new SIP Account** in the **SIP Account** screen or **Edit** icon next to an existing account.

Figure 119 SIP Account: Add/Edit



Each field is described in the following table.

Table 81 SIP Account: Edit

LABEL	DESCRIPTION
SIP Service Provider Selection	
Service Provider Selection	Select the SIP service provider profile you want to use for the SIP account you configure in this screen. This field is view-only if you are editing the SIP account.
SIP Account Selection	

Table 81 SIP Account: Edit (continued)

LABEL	DESCRIPTION
SIP Account Selection	This shows the SIP account you are configuring.
General	
SIP Account	Select the **Active SIP Account** check box if you want to use this account. Clear it if you do not want to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
Authentication	
Username	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
URL Type	
URL Type	Select whether or not to include the SIP service domain name when the Device sends the SIP number. **SIP** - include the SIP service domain name. **TEL** - do not include the SIP service domain name.
Voice Features	
Primary Compression Type Secondary Compression Type Third Compression Type	Select the type of voice coder/decoder (codec) that you want the Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). • **G.711MuLaw** is typically used in North America and Japan. • **G.711ALaw** is typically used in Europe. • **G.729** only requires 8 kbps. • **G.726-32** operates at 16, 24, 32 or 40 kbps. • **G.722** operates at 48, 56 and 64 kbps.The Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec. Select the Device's first choice for voice coder/decoder. Select the Device's second choice for voice coder/decoder. Select **None** if you only want the Device to accept the first choice. Select the Device's third choice for voice coder/decoder. Select **None** if you only want the Device to accept the first or second choice.
Speaking Volume Control	Enter the loudness that the Device uses for speech that it sends to the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.
Listening Volume Control	Enter the loudness that the Device uses for speech that it receives from the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.
Active G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD (Voice Active Detector)	Select this if the Device should stop transmitting when you are not speaking. This reduces the bandwidth the Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Active Call Transfer	Select this to enable call transfer on the Device. This allows you to transfer an incoming call (that you have answered) to another phone.

Table 81 SIP Account: Edit (continued)

LABEL	DESCRIPTION
Active Call Waiting	Select this to enable call waiting on the Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Active Call Waiting Reject Time	Specify a time of seconds that the Device waits before rejecting the second call if you do not answer it.
Active Unconditional Forward	Select this if you want the Device to forward all incoming calls to the specified phone number. Specify the phone number in the **To Number** field on the right.
Active Busy Forward	Select this if you want the Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **To Number** field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Active No Answer Forward	Select this if you want the Device to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.) Specify the phone number in the **To Number** field on the right.
No Answer Ring Time	This field is used by the **Active No Answer Forward** feature. Enter the number of seconds the Device should wait for you to answer an incoming call before it considers the call is unanswered.
Hot Line / Warm Line Enable	Select this to enable the hot line or warm line feature on the Device.
Warm Line	Select this to have the Device dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time.
Hot Line	Select this to have the Device dial the specified hot line number immediately when you pick up the telephone.
Hot Line / Warm Line number	Enter the number of the hot line or warm line that you want the Device to dial.
Warm Line Timer	Enter a number of seconds that the Device waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad.
Active Anonymous Call Block	Select this if you want the Device to bloack anonymous calls.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

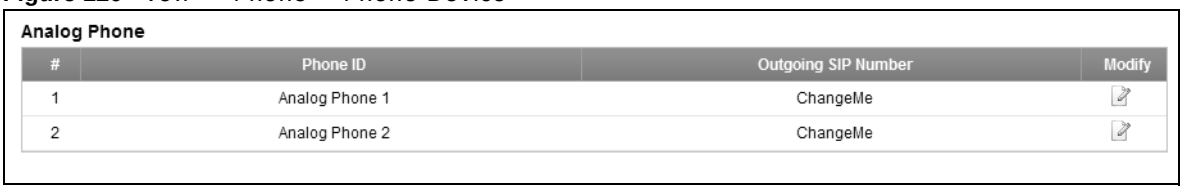
18.4 Multiple SIP Accounts

You can set up two SIP accounts on your Device and your Device is equipped with two phone ports. By default, SIP1 of the Device maps to phone port 1 for incoming and outgoing, and SIP2 maps to phone port 2 for incoming and outgoing.

18.5 Phone Screen

Use this screen to control which SIP accounts and PSTN line each phone uses. Click **VoIP > Phone** to access the **Phone Device** screen.

Figure 120 VoIP > Phone > Phone Device



The following table describes the labels in this screen.

Table 82 VoIP > Phone > Phone Device

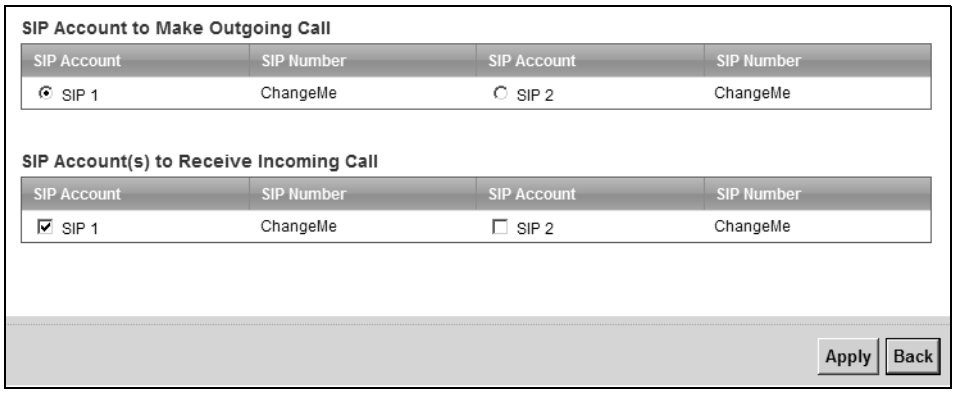
LABEL	DESCRIPTION
#	This is the index number of the entry.
Phone ID	This is the phone device number.
Outgoing SIP Number	This is the outgoing SIP number of the phone device.
Modify	Click the **Edit** icon to configure the SIP account.

18.5.1 Edit Phone Device

You can decide which SIP accounts the phones connected to the Device use by clicking the **Edit** icon next to a Phone ID. The following screen displays.

You cannot edit the account if it is not activated. Go to **VoIP > SIP > SIP Account > Edit** to activate a SIP account (see Section 18.3 on page 226 for more information).

Figure 121 Phone Device: Edit


SIP Account to Make Outgoing Call
SIP Account SIP Number SIP Account SIP Number
SIP 1 ChangeMe SIP 2 ChangeMe
SIP Account(s) to Receive Incoming Call
SIP Account SIP Number SIP Account SIP Number
SIP 1 ChangeMe SIP 2 ChangeMe
Apply
Back

The following table describes the labels in this screen.

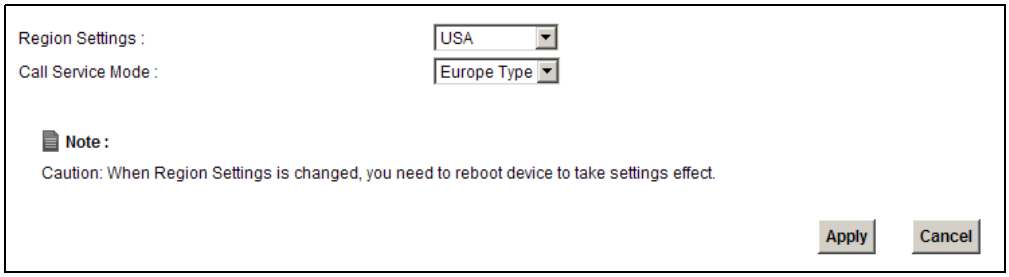
Table 83 Phone Device: Edit

LABEL	DESCRIPTION
SIP Account to Make Outgoing Call	
SIP Account	Select the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port.
SIP Number	This shows the SIP account number.
SIP Account(s) to Receive Incoming Call	
SIP Account	Select a SIP account if you want to receive phone calls for the selected SIP account on this phone port. If you select more than one SIP account for incoming calls, there is no way to distinguish between them when you receive phone calls. If you do not select a source for incoming calls, you cannot receive any calls on this phone port.
SIP Number	This shows the SIP account number.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

18.6 The Phone Region Screen

Use this screen to maintain settings that depend on which region of the world the Device is in. To access this screen, click **VoIP > Phone > Region**.

Figure 122 VoIP > Phone > Region



Each field is described in the following table.

Table 84 VoIP > Phone > Region

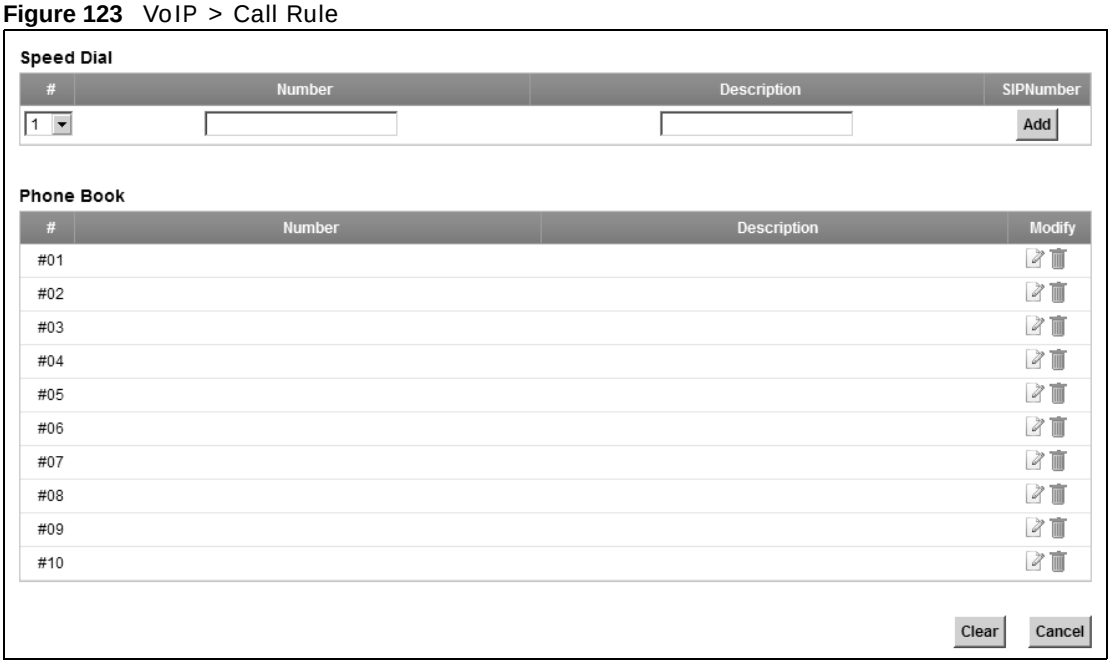
LABEL	DESCRIPTION
Region Settings	Select the place in which the Device is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. • **Europe Type** - use supplementary phone services in European mode. • **USA Type** - use supplementary phone services American mode. You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the Device.
Cancel	Click this to set every field in this screen to its last-saved value.

18.7 The Call Rule Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

To access this screen, click **VoIP > Call Rule**.

Figure 123 VoIP > Call Rule



Each field is described in the following table.

Table 85 VoIP > Call Rule

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Add	Click this to use the information in the **Speed Dial** section to update the **Speed Dial Phone Book** section.
Phone Book	Use this section to look at all the speed-dial entries and to erase them.
#	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the Device calls when you dial the speed-dial number.
Description	This field displays a short description of the party you call when you dial the speed-dial number.

Table 85 VoIP > Call Rule (continued)

LABEL	DESCRIPTION
Modify	Use this field to edit or erase the speed-dial entry. Click the **Edit** icon to copy the information for this speed-dial entry into the **Speed Dial** section, where you can change it. Click **Add** when you finish editing to change the configurations. Click the **Delete** icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.
Cancel	Click this to set every field in this screen to its last-saved value.

18.8 Technical Reference

This section contains background material relevant to the **VoIP** screens.

18.8.1 VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

18.8.2 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

SIP Registration

Each Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the Device attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC3261, "SIP: Session Initiation Protocol").

SIP Servers

SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

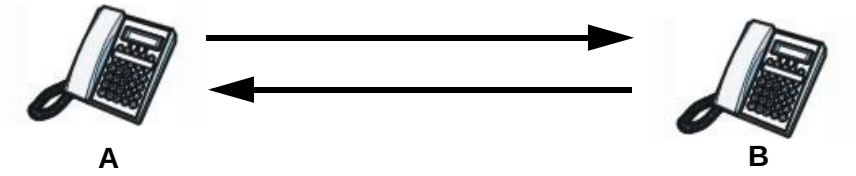
When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure,

either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

Figure 124 SIP User Agent



SIP Proxy Server

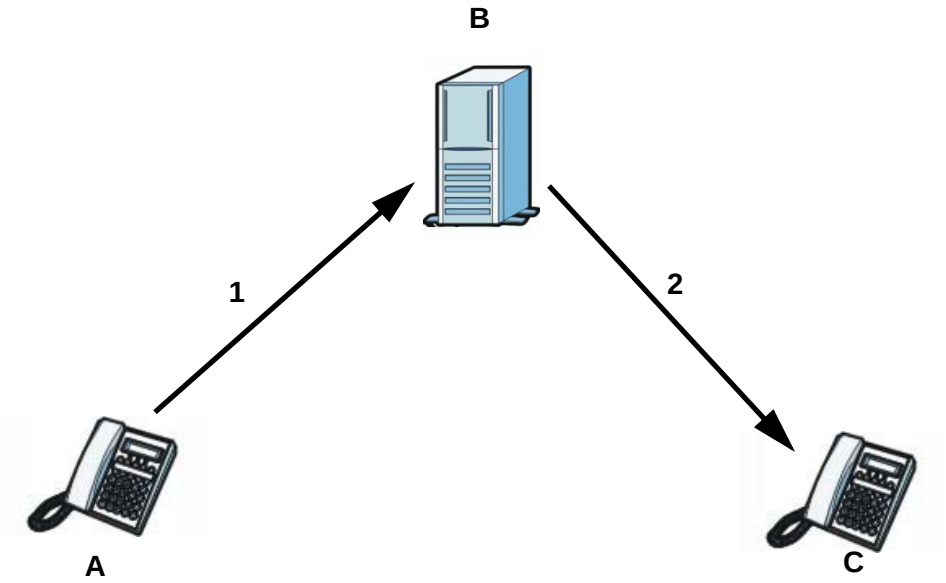
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server **B**.

2 The SIP proxy server forwards the call invitation to **C**.

Figure 125 SIP Proxy Server



SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

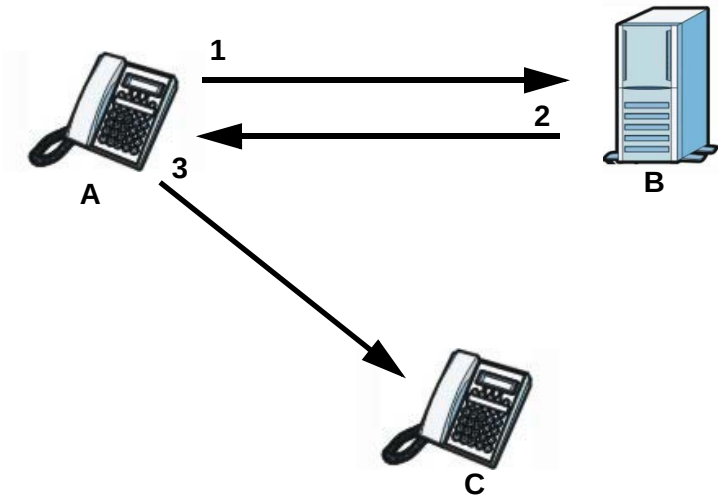
In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 Client device **A** sends a call invitation for **C** to the SIP redirect server **B**.

2 The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).

3 Client device **A** then sends the call invitation to client device **C**.

Figure 126 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 3550 for details on RTP.

Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 86 SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	

Table 86 SIP Call Progression (continued)

A		B
	5.Dialogue (voice traffic)	
6. BYE		
		7. OK

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

PSTN Call Setup Signaling

Dual-Tone MultiFrequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.[3]

3. The Device does not support pulse dialing at the time of writing.

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

18.8.3 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

DiffServ

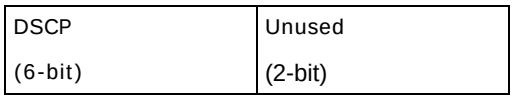
DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[4]

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 127 DiffServ: Differentiated Service Field



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

4. The Device does not support DiffServ at the time of writing.

VLAN Tagging

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your Device can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the Device to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

18.8.4 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Three-Way Conference
- Internal Calls
- Do not Disturb

Note: To take full advantage of the supplementary phone services available through the Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the Device.

You can invoke all the supplementary services by using the flash key.

Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command time-out (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 87 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press “0”.
- Disconnect the first call and answer the second call.

  Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then “2”.

European Call Transfer

Do the following to transfer a call (that you have answered) to another phone number.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call. to operate the Intercom.
3. After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, press the flash key to put the call on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press “3” to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

19

Logs

19.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the Device log and then display the logs or have the Device send them to an administrator (as e-mail) or to a syslog server.

19.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs for the categories that you select (Section 19.2 on page 244).
- Use the **Phone Log** screen to view phone logs and alert messages (Section 19.3 on page 245).
- Use The **VoIP Call History** screen to view the details of the calls performed on the Device (Section 19.4 on page 245).

19.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 88 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.

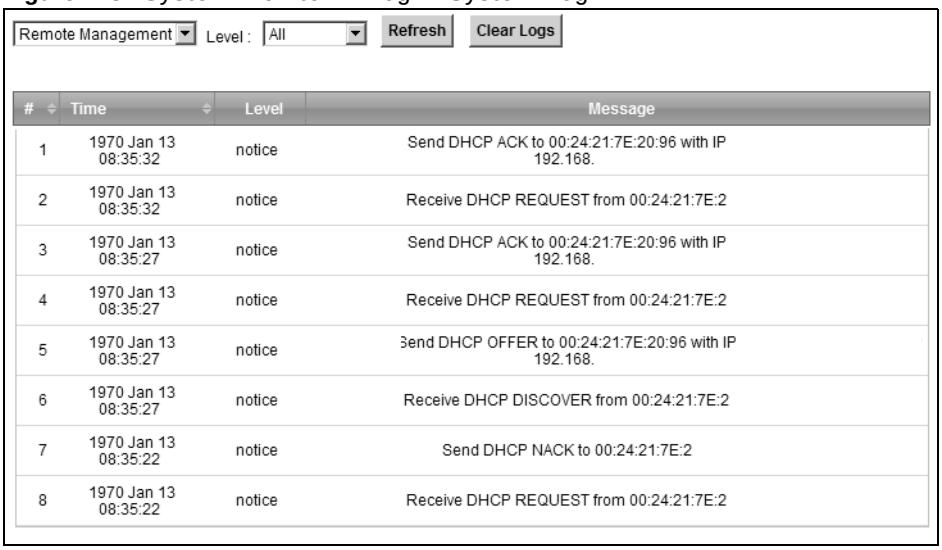
Table 88 Syslog Severity Levels

CODE	SEVERITY
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

19.2 The System Log Screen

Click **System Monitor > Log** to open the **System Log** screen. Use the **System Log** screen to see the system logs for the categories that you select in the upper left drop-down list box.

Figure 128 System Monitor > Log > System Log


Remote Management
Level :
All
Refresh
Clear Logs
Time Level Message
1 1970 Jan 13 08:35:32 notice Send DHCP ACK to 00:24:21:7E:20:96 with IP 192.168.
2 1970 Jan 13 08:35:32 notice Receive DHCP REQUEST from 00:24:21:7E:2
3 1970 Jan 13 08:35:27 notice Send DHCP ACK to 00:24:21:7E:20:96 with IP 192.168.
4 1970 Jan 13 08:35:27 notice Receive DHCP REQUEST from 00:24:21:7E:2
5 1970 Jan 13 08:35:27 notice Send DHCP OFFER to 00:24:21:7E:20:96 with IP 192.168.
6 1970 Jan 13 08:35:27 notice Receive DHCP DISCOVER from 00:24:21:7E:2
7 1970 Jan 13 08:35:22 notice Send DHCP NACK to 00:24:21:7E:2
8 1970 Jan 13 08:35:22 notice Receive DHCP REQUEST from 00:24:21:7E:2

The following table describes the fields in this screen.

Table 89 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Device searches through all logs of that severity or higher.
Refresh	Click this to renew the log screen.
Clear Log	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

19.3 The Phone Log Screen

Click **System Monitor > Log** to open the **Phone Log** screen. Use this screen to view phone logs and alert messages. You can select the type of log and level of severity to display.

Figure 129 System Monitor > Log > Phone Log

AllLogs
Level :
All
Refresh
Clear Logs
Time Level Message
1 Aug 20 07:37:17 err SIP Registration: SIP:12875: Register Fail, error_cause 43
2 Aug 20 07:37:40 info [ChangeMe] [FXS2] Phone Event: OFFHOOK
3 Aug 20 07:37:43 info [ChangeMe] [FXS2] Phone Event: ONHOOK
4 Aug 20 07:37:43 info [ChangeMe] [FXS2] Phone Event: idle
5 Aug 20 07:39:05 info [ChangeMe] [FXS2] Phone Event: OFFHOOK
6 Aug 20 07:39:28 info [ChangeMe] [FXS2] Phone Event: ONHOOK
7 Aug 20 07:39:28 info [ChangeMe] [FXS2] Phone Event: idle
8 Aug 20 07:41:14 info SIP Registration: SIP:128752: Register Success
9 Aug 20 07:41:49 info [ChangeMe] [FXS2] Phone Event: OFFHOOK
10 Aug 20 07:41:56 info [ChangeMe] [FXS2] Phone Event: ONHOOK

The following table describes the fields in this screen.

Table 90 System Monitor > Log > Phone Log

LABEL	DESCRIPTION
	Select a category of logs to view from the drop-down list box. select **All Logs** to view all logs.
Level	Select the severity level that you want to view.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Message	This field states the reason for the log.

19.4 The VoIP Call History Screen

Click **System Monitor > Log > VoIP Call History** to open the **VoIP Call History** screen. Use this screen to see the details of the calls performed on the Device.

Figure 130 System Monitor > Log > VoIP Call History

The following table describes the fields in this screen.

Table 91 System Monitor > Log > VoIP Call History

LABEL	DESCRIPTION
	Select a category of call records to view from the drop-down list box. select **All Call History** to view all call records.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the call was recorded.
Local Number	This field displays the phone number you used to make or receive this call.
Peer Number	This field displays the phone number you called or from which this call is made.
Interface	This field displays the type of the call.
Duration	This field displays how long the call lasted.

20

Traffic Status

20.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

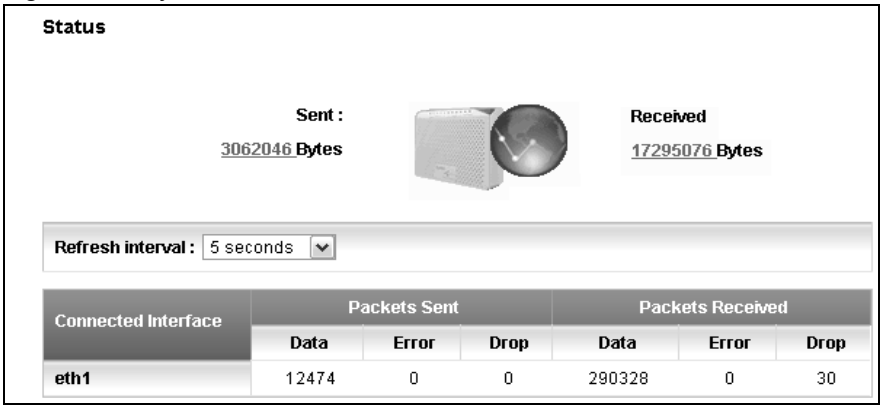
20.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 20.2 on page 247) .
- Use the **LAN** screen to view the LAN traffic statistics (Section 20.3 on page 248).
- Use the **NAT** screen to view the NAT status of the Device's client(s) (Section 20.4 on page 249).
- Use the **3G Backup** screen to view the 3G connection traffic statistics (Section 20.6 on page 251).
- Use the **VoIP Status** screen to view the VoIP traffic statistics (Section 20.6 on page 251).

20.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. You can view the WAN traffic statistics in this screen.

Figure 131 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 92 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Status	This shows the number of bytes received and sent through the WAN interface of the Device.
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.

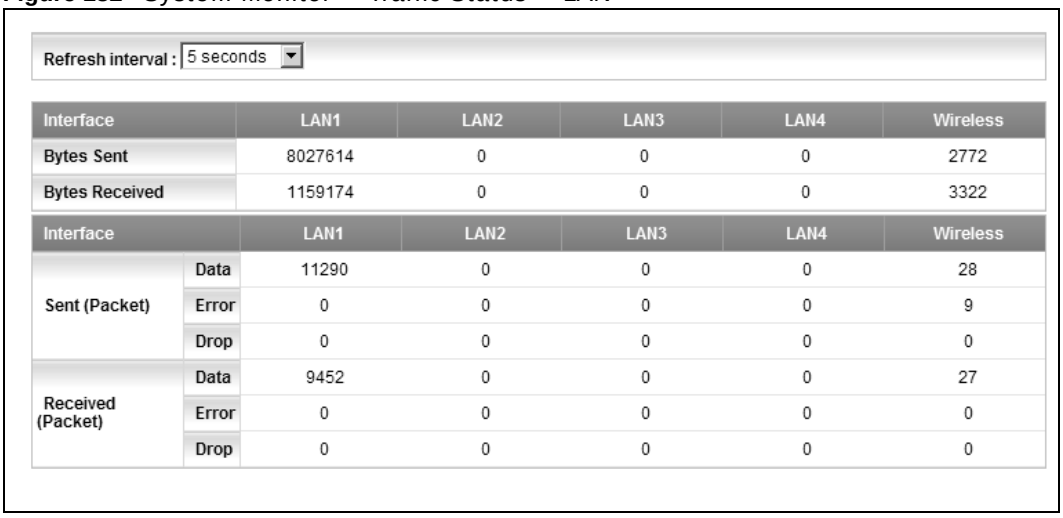
Table 92 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

20.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. You can view the LAN traffic statistics in this screen.

Figure 132 System Monitor > Traffic Status > LAN


Refresh interval : 5 seconds
Interface LAN1 LAN2 LAN3 LAN4 Wireless
Bytes Sent 8027614 0 0 0 2772
Bytes Received 1159174 0 0 0 3322
Interface LAN1 LAN2 LAN3 LAN4 Wireless
Sent (Packet) Data 11290 0 0 0 28
Error 0 0 0 0 9
Drop 0 0 0 0 0
Received (Packet) Data 9452 0 0 0 27
Error 0 0 0 0 0
Drop 0 0 0 0 0

The following table describes the fields in this screen.

Table 93 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interface.
Sent (Packet)	
Data	This indicates the number of transmitted packets on this interface.

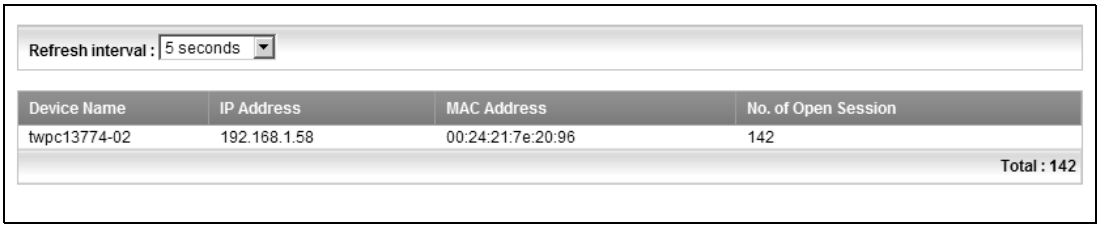
Table 93 System Monitor > Traffic Status > LAN (continued)

LABEL	DESCRIPTION
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packet)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

20.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. You can view the NAT status of the Device's client(s) in this screen.

Figure 133 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

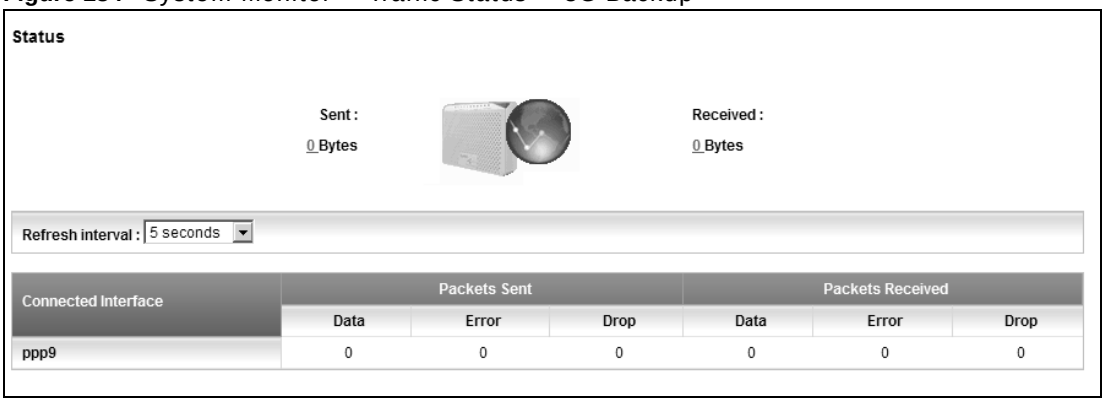
Table 94 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Device Name	This shows the name of the client.
IP Address	This shows the IP address of the client.
MAC Address	This shows the MAC address of the client.
No. of Open Session	This shows the number of NAT sessions used by the client.

20.5 The 3G Backup Status Screen

Click **System Monitor > Traffic Status > 3G Backup** to open the following screen. You can view the 3G connection traffic statistics in this screen.

Figure 134 System Monitor > Traffic Status > 3G Backup



The following table describes the fields in this screen.

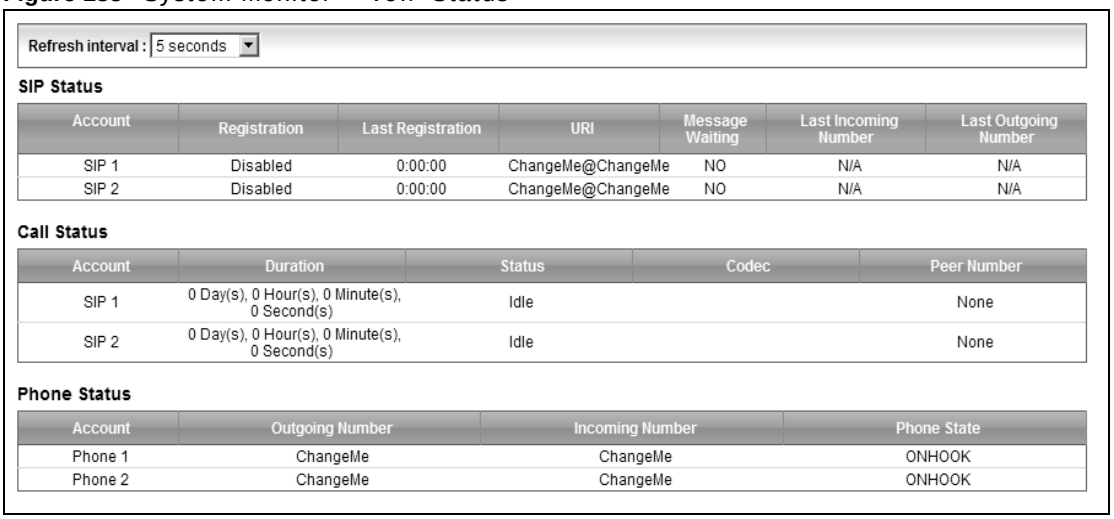
Table 95 System Monitor > Traffic Status > 3G backup

LABEL	DESCRIPTION
Status	This shows the number of bytes received and sent through the 3G interface of the Device.
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Connected Interface	This shows the name of the 3G connection interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

20.6 The VoIP Status Screen

Click **System Monitor > VoIP Status** to open the following screen. You can view the VoIP traffic statistics in this screen.

Figure 135 System Monitor > VoIP Status



The following table describes the fields in this screen.

Table 96 System Monitor > VoIP Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
SIP Status	
Account	This column displays each SIP account in the Device.
Registration	This field displays the current registration status of the SIP account. You can change this in the **Status** screen. **Registered** - The SIP account is registered with a SIP server. **Not Registered** - The last time the Device tried to register the SIP account with the SIP server, the attempt failed. The Device automatically tries to register the SIP account when you turn on the Device or when you activate it. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Account**.
Last Registration	This field displays the last time you successfully registered the SIP account. The field is blank if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP > SIP** screens.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the Device.
Duration	This field displays how long the current call has lasted.

Table 96 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Status	This field displays the current state of the phone call. **Idle** - There are no current VoIP calls, incoming calls or outgoing calls being made. **Dial** - The callee's phone is ringing. **Ring** - The phone is ringing for an incoming VoIP call. **Process** - There is a VoIP call in progress. **DISC** - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Account	This field displays the phone accounts of the Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Phone State	This field shows whether or the phone connected to the subscriber port is on-hook **ONHOOK**) or off-hook **(OFFHOOK**).

21

User Account

21.1 Overview

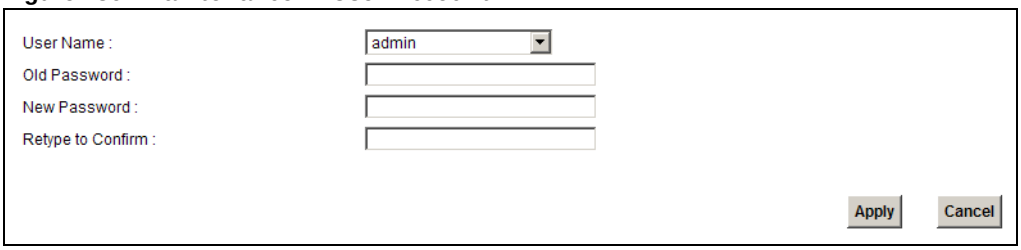
You can configure system password for different user accounts in the **User Account** screen.

21.2 The User Account Screen

Use the **User Account** screen to configure system password.

Click **Maintenance > User Account** to open the following screen.

Figure 136 Maintenance > User Account



The following table describes the labels in this screen.

Table 97 Maintenance > User Account

LABEL	DESCRIPTION
User Name	You can configure the password for the **Admin** and **User** accounts.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

22

Remote MGMT

22.1 Overview

Remote MGMT allows you to manage your Device from a remote location through the following interfaces:

- LAN and WLAN
- WAN only

Note: The Device is managed using the web configurator.

22.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter

TR-064

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

SSH/SCP/SFTP

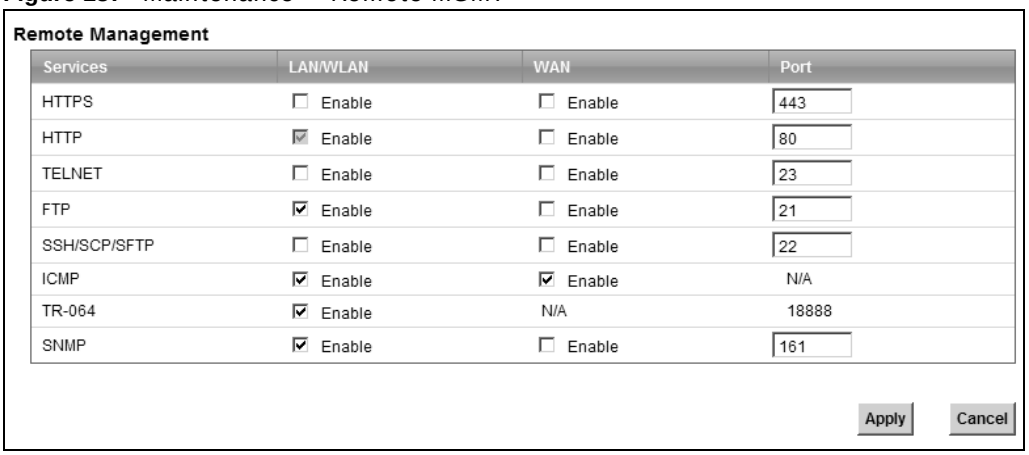
Secure Shell (SSH) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. The following file transfer methods use SSH:

- **Secure Copy (SC)** is a secure way of transferring files between computers. It uses port 22.
- **SSH File Transfer Protocol or Secure File Transfer Protocol (SFTP)** is an old way of transferring files between computers. It uses port 22.

22.2 The Remote MGMT Screen

Use this screen to decide what services you may use to access which Device interface. Click **Maintenance > Remote MGMT** to open the following screen.

Figure 137 Maintenance > Remote MGMT



The following table describes the fields in this screen.

Table 98 Maintenance > Remote MGMT

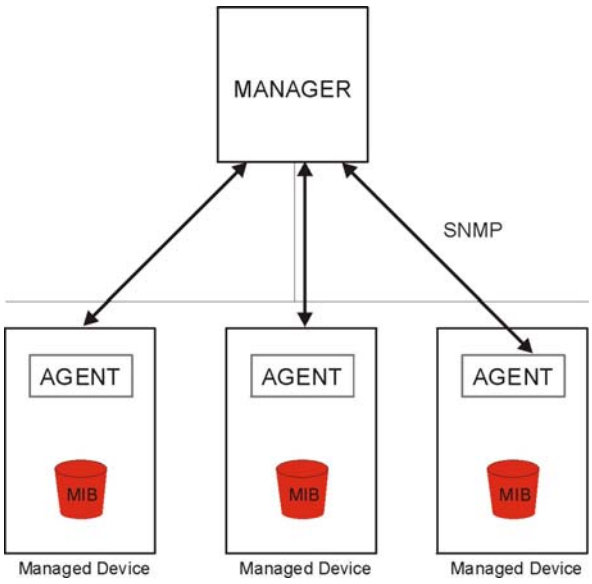
LABEL	DESCRIPTION
Services	This is the service you may use to access the Device.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Device from the LAN and WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Device from the WAN.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

23

The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Device through the network. The Device supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 138 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

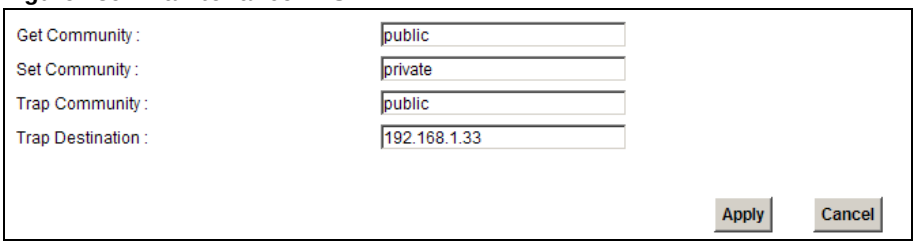
SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.

- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

To change your Device's SNMP settings, click **Maintenance** > **SNMP** to display the screen as shown.

Figure 139 Maintenance > SNMP



The following table describes the labels in this screen.

Table 99 Configuration > Management > Remote MGMT > SNMP

LABEL	DESCRIPTION
Get Community	Enter the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

24 System

24.1 Overview

You can configure system settings, including the host name, domain name and the inactivity time-out interval in the **System** screen.

24.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter.

Domain Name

This is a network address that identifies the owner of a network connection. For example, in the network address “www.zyxel.com/support/files”, the domain name is “www.zyxel.com”.

24.2 The System Screen

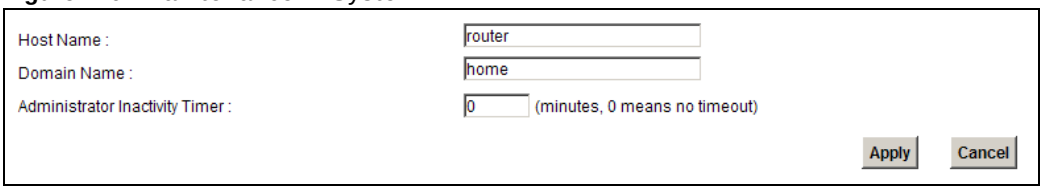
Use the **System** screen to configure the system’s host name, domain name, and inactivity time-out interval.

The **Host Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer.

In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Device **System Name**.

Click **Maintenance > System** to open the following screen.

Figure 140 Maintenance > System



The following table describes the labels in this screen.

Table 100 Maintenance > System

LABEL	DESCRIPTION
Host Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click this to save your changes back to the Device.
Cancel	Click this to begin configuring this screen afresh.

25

Time Setting

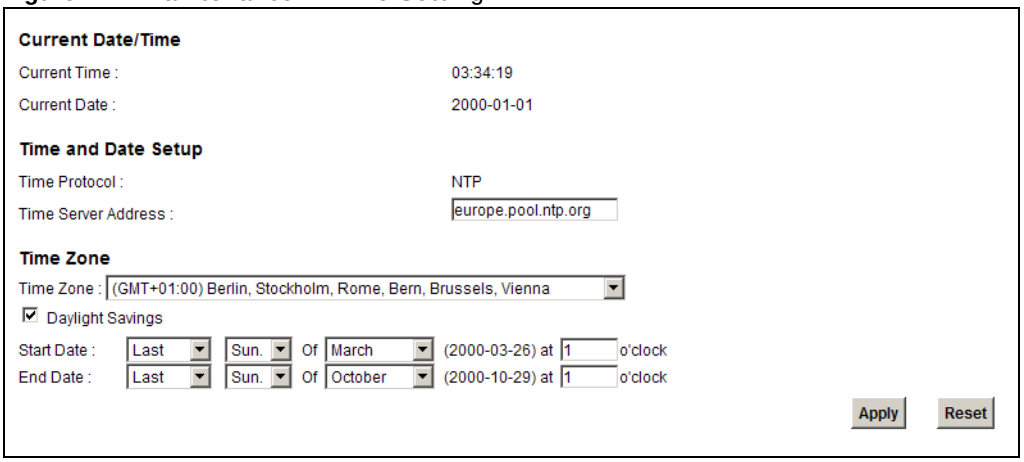
25.1 Overview

You can configure the system's time and date in the **Time Setting** screen.

25.2 The Time Setting Screen

To change your Device's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the Device's time based on your local time zone.

Figure 141 Maintenance > Time Setting



The following table describes the fields in this screen.

Table 101 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your Device.
Current Date	This field displays the date of your Device.
Time and Date Setup	
Time Protocol	This shows the time service protocol that your time server sends when you turn on the Device.
Time Server Address	Enter the IP address or URL (up to 31 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Table 101 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type **2** in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type **2** in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

26

Log Setting

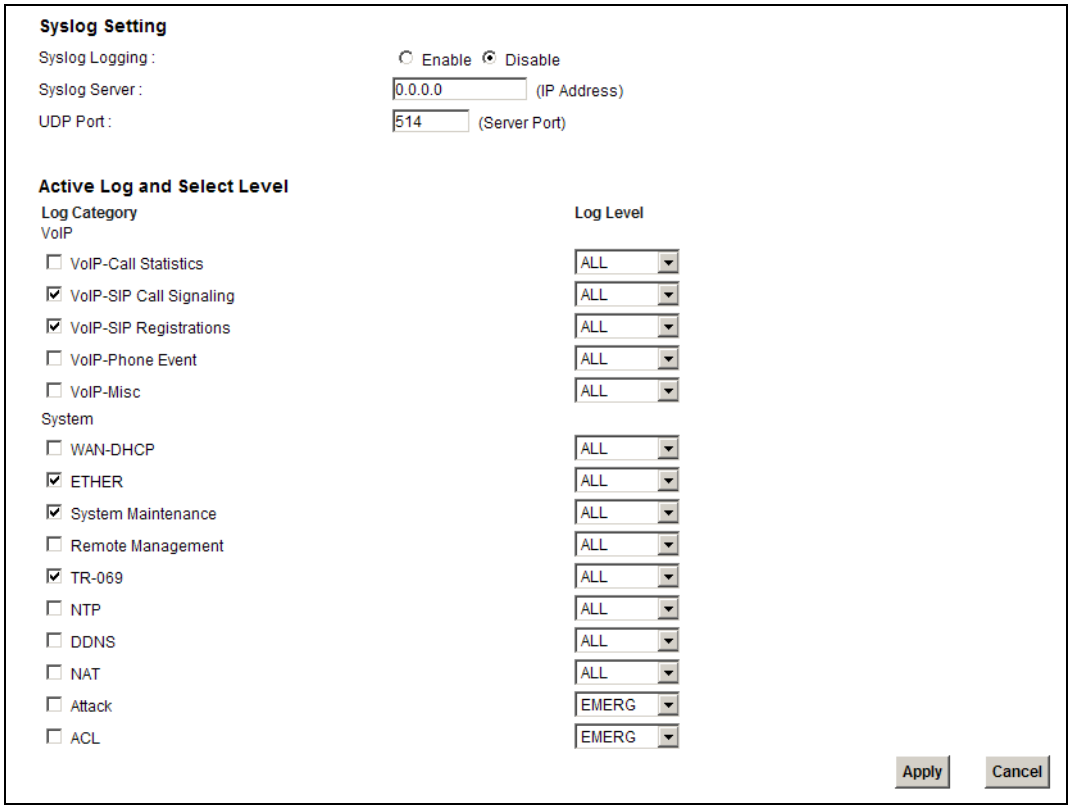
26.1 Overview

You can configure where the Device sends logs and which logs and/or immediate alerts the Device records in the **Log Setting** screen.

26.2 The Log Setting Screen

To change your Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 142 Maintenance > Log Setting



The following table describes the fields in this screen.

Table 102 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The Device sends a log to an external syslog server. Select the **Enable** check box to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
Active Log and Select Level	
Log Category	Select the categories of logs that you want to record.
Log Level	Select the severity level of logs that you want to record. If you want to record all logs, select **ALL**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

27

Firmware Upgrade

27.1 Overview

This chapter explains how to upload new firmware to your Device. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

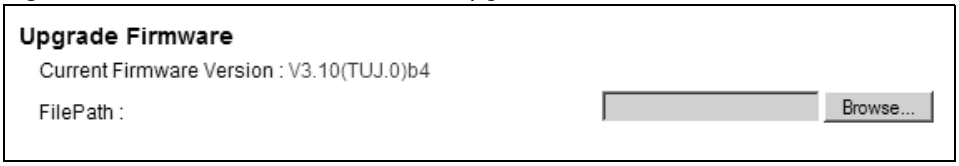
Only use firmware for your device's specific model. Refer to the label on the bottom of your Device.

27.2 The Firmware Upgrade Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the system will reboot.

Do NOT turn off the Device while firmware upload is in progress!

Figure 143 Maintenance > Firmware Upgrade



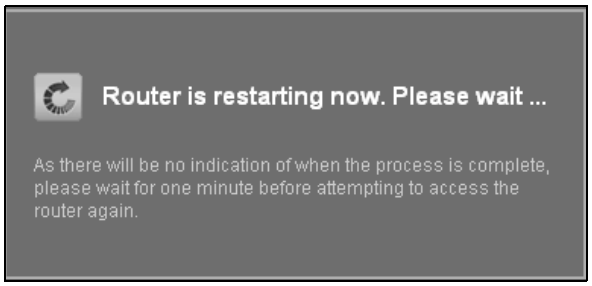
The following table describes the labels in this screen.

Table 103 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to three minutes.

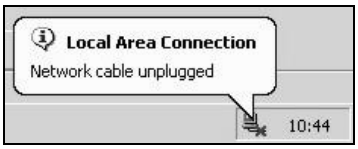
After you see the firmware updating screen, wait a few minutes before logging into the Device again.

Figure 144 Firmware Uploading


Router is restarting now. Please wait ...
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

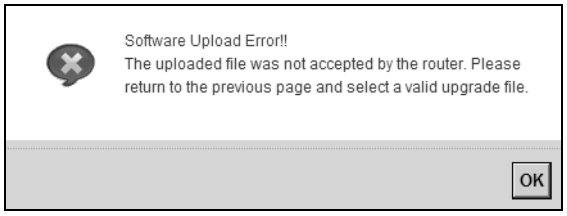
Figure 145 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 146 Error Message


Software Upload Error!!
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file.
OK

28

Backup/Restore

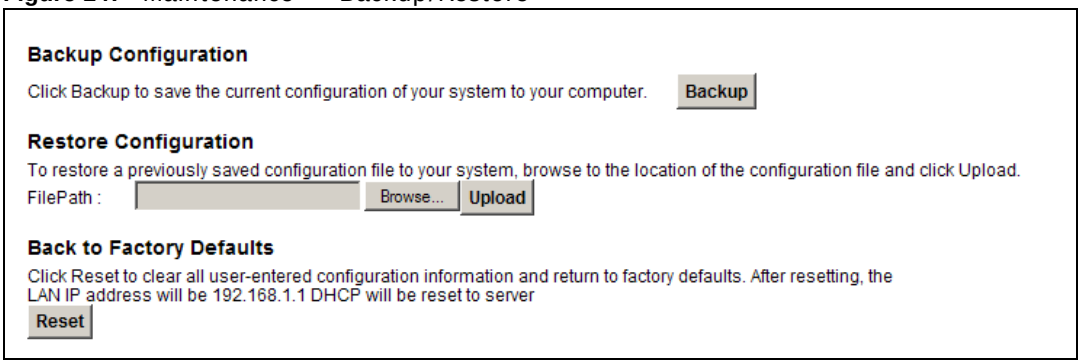
28.1 Overview

The **Backup / Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

28.2 The Backup/Restore Screen

Click **Maintenance > Backup / Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 147 Maintenance > Backup/Restore


Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
FilePath :
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the LAN IP address will be 192.168.1.1 DHCP will be reset to server
Reset

Backup Configuration

Backup Configuration allows you to back up (save) the Device's current configuration to a file on your computer. Once your Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your Device.

Table 104 Restore Configuration

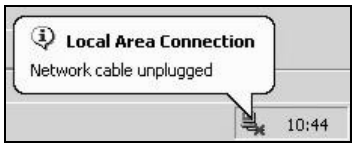
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your device settings back to the factory default.

Do not turn off the Device while configuration file upload is in progress.

After the Device configuration has been restored successfully, the login screen appears. Login again to restart the Device.

The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 148 Network Temporarily Disconnected



If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix B on page 293 for details on how to set up your computer's IP address.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the Device to its factory defaults. The following warning screen appears.

Figure 149 Reset Warning Message

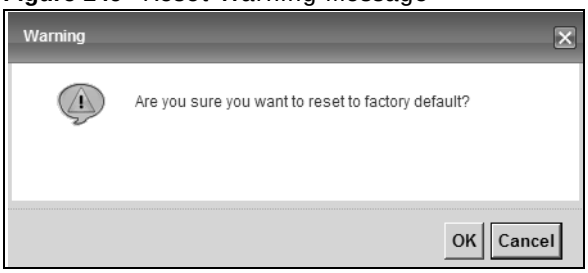
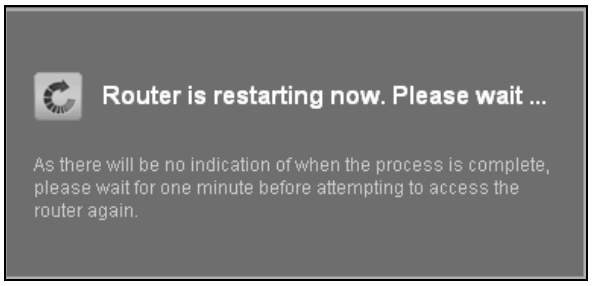


Figure 150 Reset In Process Message


Router is restarting now. Please wait ...
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

You can also press the **RESET** button on the back panel to reset the factory defaults of your Device. Refer to Section 1.7 on page 22 for more information on the **RESET** button.

28.3 The Reboot Screen

System restart allows you to reboot the Device remotely without turning the power off. You may need to do this if the Device hangs, for example.

Click **Maintenance > Reboot**. Click the **Reboot** button to have the Device reboot. This does not affect the Device's configuration.

29

Diagnostic

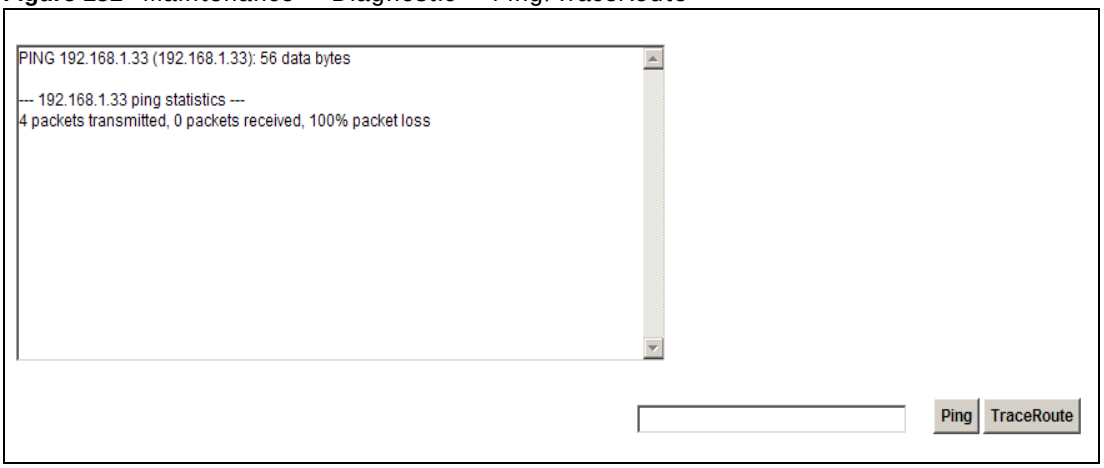
29.1 Overview

You can use different diagnostic methods to test a connection and see the detailed information. These read-only screens display information to help you identify problems with the Device.

29.2 The Ping/TraceRoute Screen

Ping and traceroute help check availability of remote hosts and also help troubleshoot network or Internet connections. Click **Maintenance > Diagnostic** to open the **Ping / TraceRoute** screen shown next.

Figure 151 Maintenance > Diagnostic > Ping/TraceRoute


PING 192.168.1.33 (192.168.1.33): 56 data bytes
--- 192.168.1.33 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
Ping
TraceRoute

The following table describes the fields in this screen.

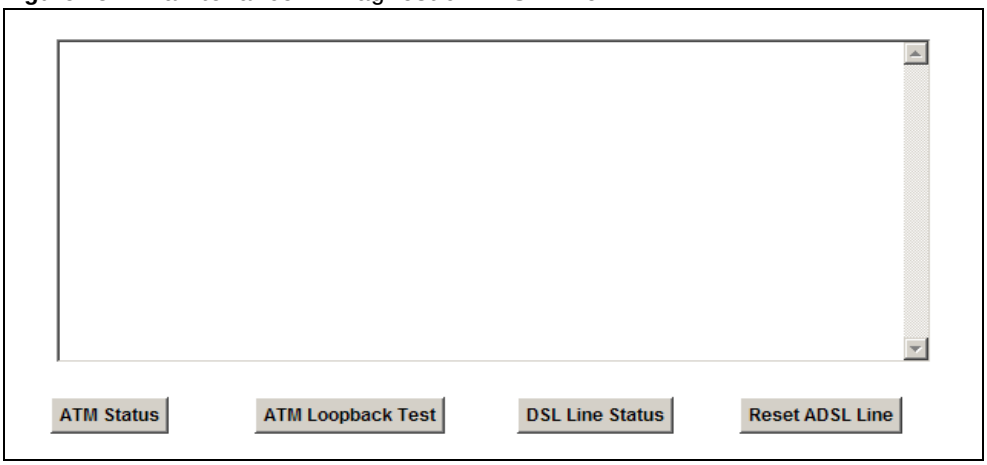
Table 105 Maintenance > Diagnostic > Ping/TraceRoute

LABEL	DESCRIPTION
Ping	Type the IP address of a computer that you want to ping in order to test a connection. Click **Ping** and the ping statistics will show in the diagnostic .
TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

29.3 The DSL Line Screen

Click **Maintenance > Diagnostic > DSL Line** to open the screen shown next.

Figure 152 Maintenance > Diagnostic > DSL Line



The following table describes the fields in this screen.

30

Troubleshooting

30.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Device Access and Login
- Internet Access
- Wireless Internet Access
- Phone Calls and VoIP
- USB Device Connection
- UPnP

30.2 Power, Hardware Connections, and LEDs

The Device does not turn on. None of the LEDs turn on.

1. Make sure the Device is turned on.
2. Make sure you are using the power adaptor or cord included with the Device.
3. Make sure the power adaptor or cord is connected to the Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.6 on page 20.
2. Check the hardware connections. See the Quick Start Guide.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the Device off and on.

5 If the problem continues, contact the vendor.

30.3 Device Access and Login

I forgot the IP address for the Device.

1 The default IP address is 192.168.1.1.

2 If you changed the IP address and have forgotten it, you might get the IP address of the Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.7 on page 22.

I forgot the password.

1 The default admin password is **1234** and the default user password is **1234**.

2 If you can't remember the password, you have to reset the device to its factory defaults. See Section 1.7 on page 22.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section on page 133), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix C on page 323.

4 Reset the device to its factory defaults, and try to access the Device with the default IP address. See Section 1.7 on page 22.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Device using another service, such as Telnet. If you can access the Device, check the remote management settings and firewall rules to find out why the Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the Device.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the Device. Log out of the Device in the other session, or ask the person who is logged in to log out.

3 Turn the Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 30.2 on page 273.

I cannot Telnet to the Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

30.4 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.6 on page 20.
2. Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4. If you are trying to access the Internet wirelessly, make sure you have enabled the wireless LAN by the **WPS/WLAN** button or the **Network Setting > Wireless > General** screen.
5. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
6. If the problem continues, contact your ISP.

I cannot access the Internet through an Ethernet WAN connection.

7. Make sure you connect the Ethernet WAN port to a DSL modem or router in your network.
8. Make sure you configured a proper Ethernet WAN connection with the Internet account information provided by your ISP.
9. If you set up a WAN connection using bridging service (all LAN ports and WLAN BSSs are bridged to one WAN connection), make sure you turn off the DHCP feature in the **Home Networking** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot create multiple connections of the same type.

Your WAN interface must enable VLAN and fill each WAN connection with different VLAN IDs.

I cannot access the Internet anymore. I had access to the Internet (with the Device), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.6 on page 20.
2. Turn the Device off and on.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.6 on page 20. If the Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Turn the Device off and on.

3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

30.5 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What wireless security modes does my Device support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your ZyXEL device are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2:** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA:** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

30.6 Phone Calls and VoIP

The telephone port won't work or the telephone lacks a dial tone.

1. Check the telephone connections and telephone wire.

I can access the Internet, but cannot make VoIP calls.

1. The **PHONE** light should come on. Make sure that your telephone is connected to the **PHONE** port.
2. You can also check the VoIP status in the **System Info** screen.
3. If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

30.7 USB Device Connection

The Device fails to detect my USB device.

1. Disconnect the USB device.
2. Reboot the Device.
3. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
4. Re-connect your USB device to the Device.

30.8 UPnP

When using UPnP and the Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1. Disconnect the Ethernet cable from the Device's LAN port or from your computer.
2. Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1. Wait more than three minutes.
2. Restart the applications.

31

Wall-mounting Instructions

Do the following to hang your Device on a wall.

Note: See Table 155 on page 282 for the size of screws to use and how far apart to place them.

1 Align the holes on the back of the supplied wall-mounting bracket with the screws. on the wall.

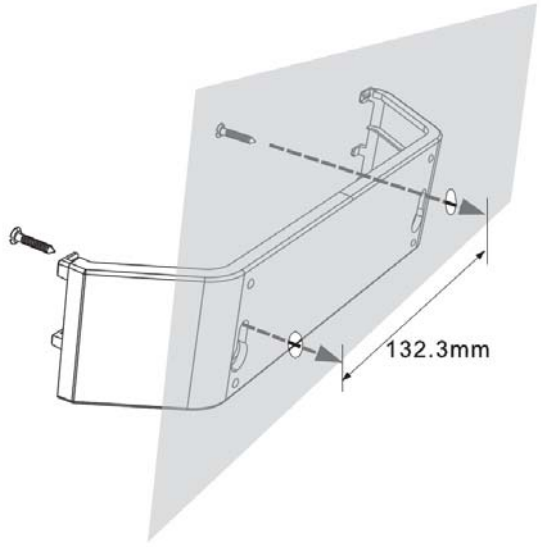
2 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.

3 Drill two holes on the wall with screws inserted in the wall-mounting bracket. The distance between the screws is 132.3mm.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

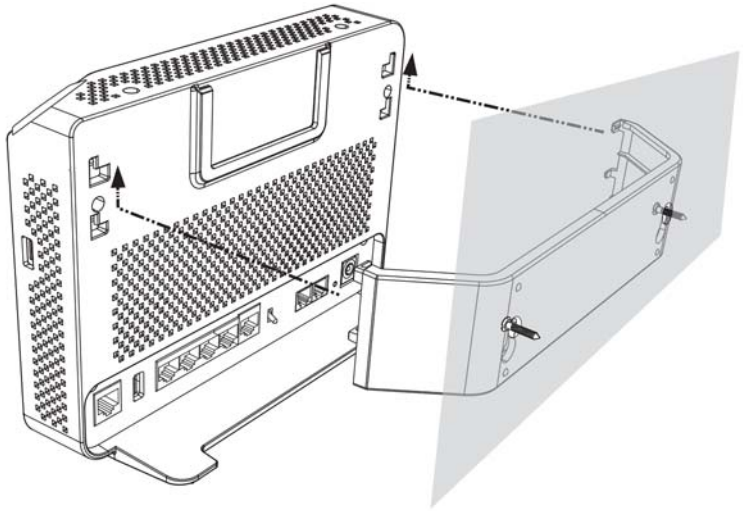
4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the Device with the connection cables.

Figure 153 Wall-mounting -1



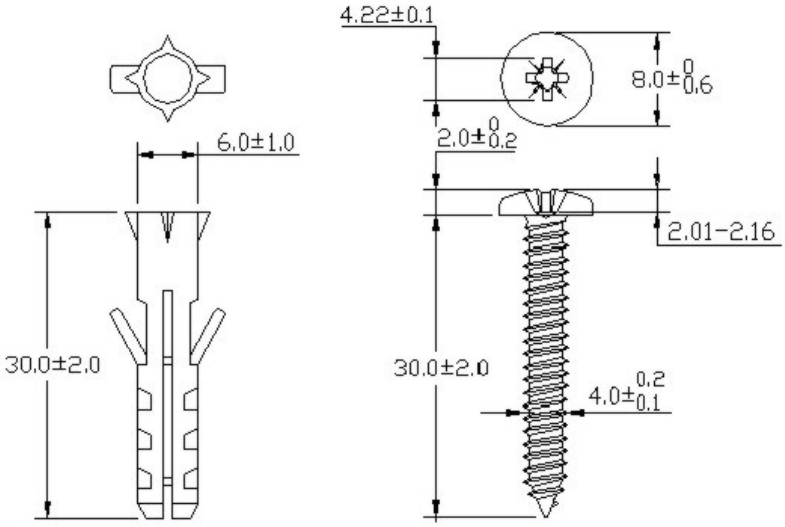
5 Mount the Device on the wall-mounting bracket, which is already installed on the wall. Make sure that the Device is firmly attached to the bracket so it does not fall off.

Figure 154 Wall-mounting -2



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 155 Masonry Plug and M4 Tap Screw



A

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (such as computers, servers, routers, and printers) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

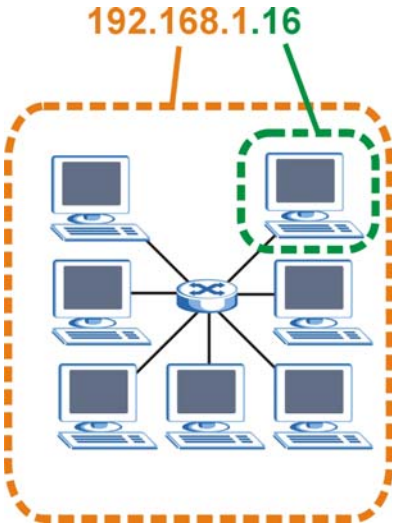
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 156 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 106 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 107 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 108 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 109 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

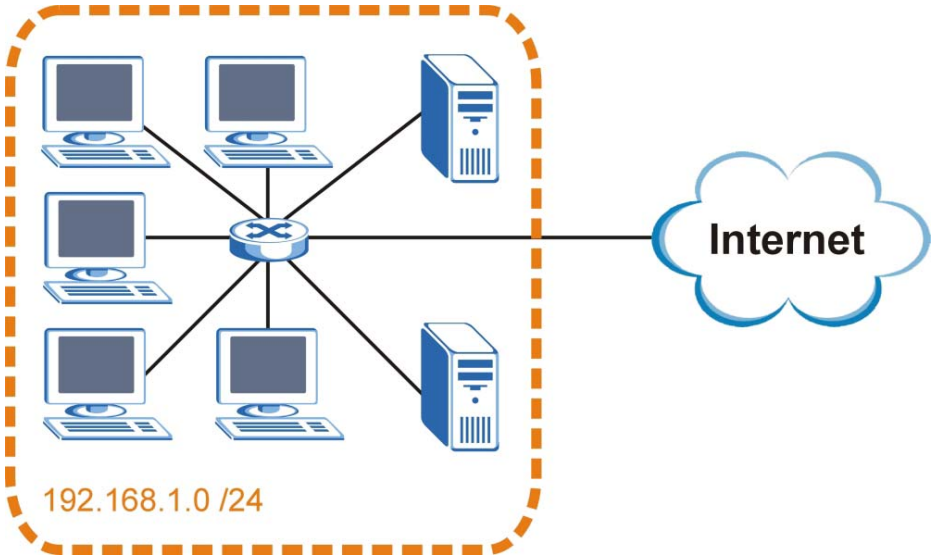
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 157 Subnetting Example: Before Subnetting

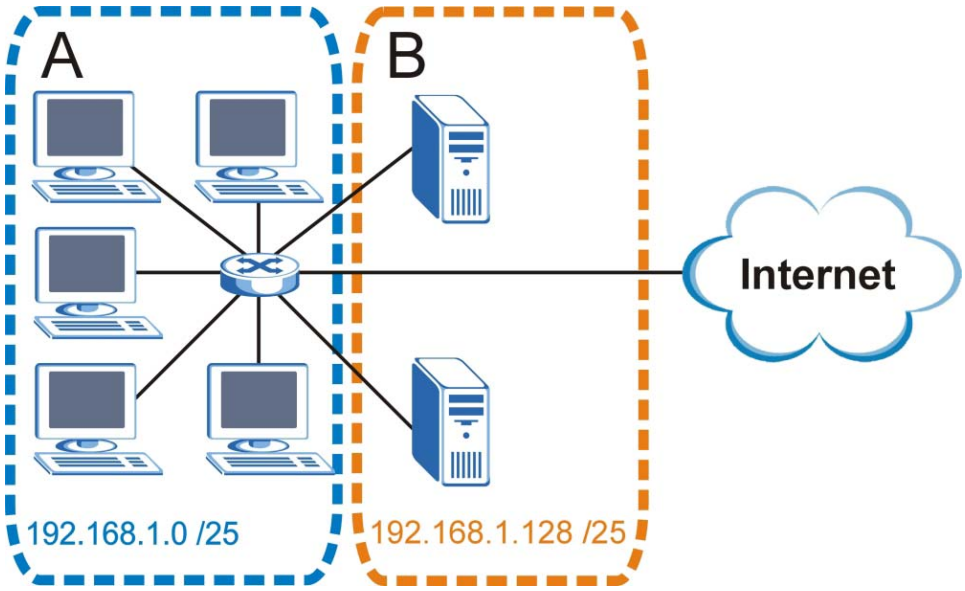


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 158 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 110 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 110 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 111 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 112 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 113 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 114 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 115 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 116 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14

Table 116 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Device.

Once you have decided on the network number, pick an IP address for your Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

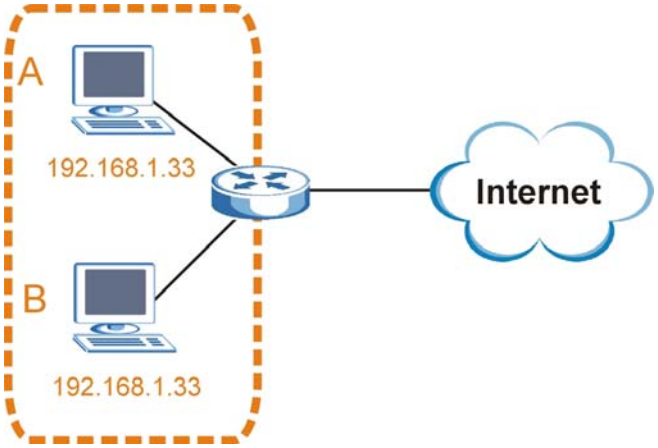
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

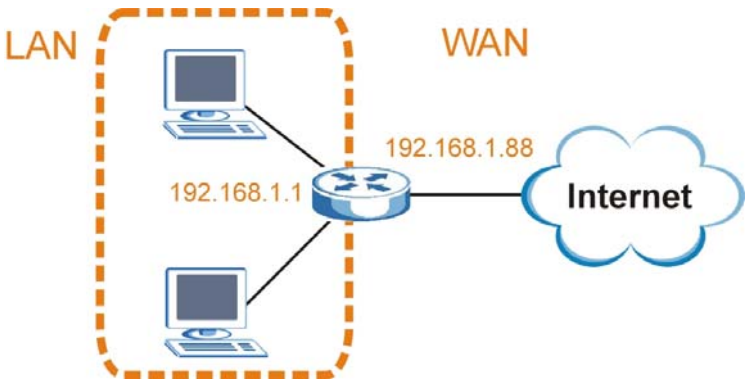
Figure 159 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

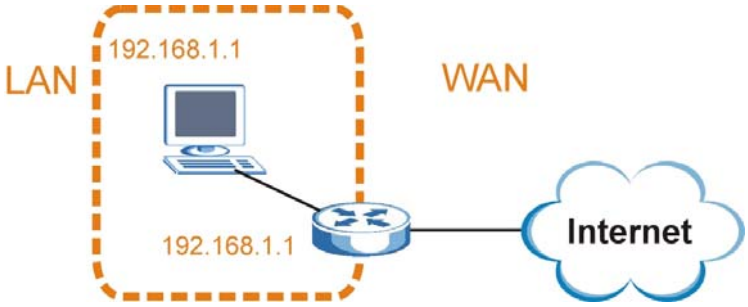
Figure 160 Conflicting Computer IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 161 Conflicting Computer and Router IP Addresses Example



B

Setting Up Your Computer's IP Address

Note: Your specific Device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

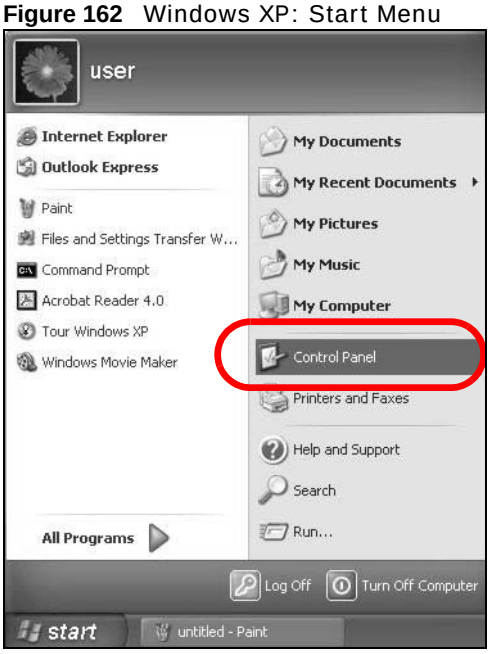
- Windows XP/NT/2000 on page 293
- Windows Vista on page 297
- Windows 7 on page 301
- Mac OS X: 10.3 and 10.4 on page 305
- Mac OS X: 10.5 on page 308
- Linux: Ubuntu 8 (GNOME) on page 312
- Linux: openSUSE 10.3 (KDE) on page 316

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

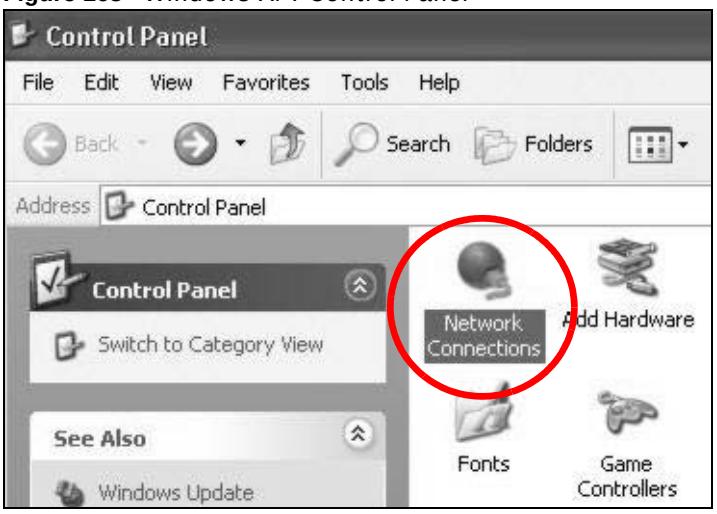
1 Click **Start** > **Control Panel**.

Figure 162 Windows XP: Start Menu



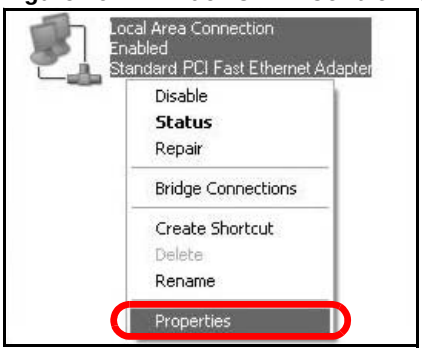
2 In the **Control Panel**, click the **Network Connections** icon.

Figure 163 Windows XP: Control Panel



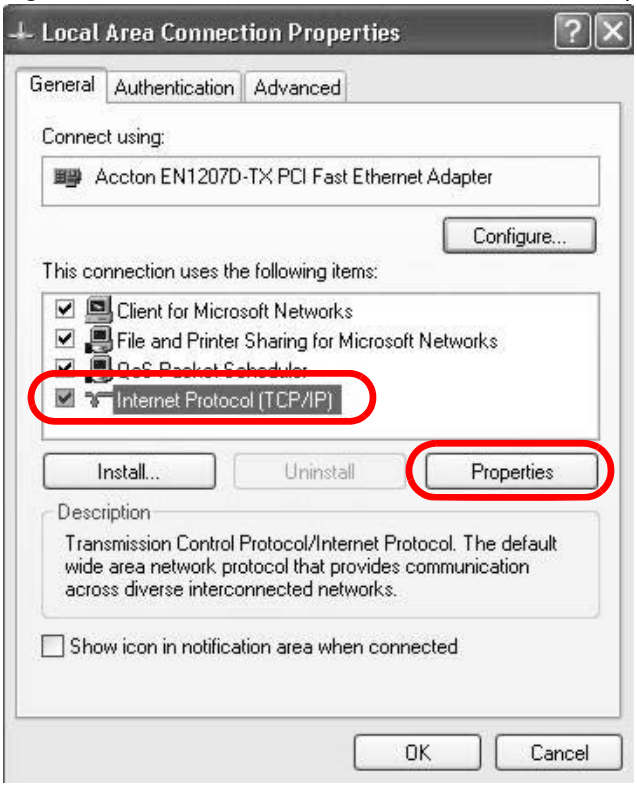
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 164 Windows XP: Control Panel > Network Connections > Properties



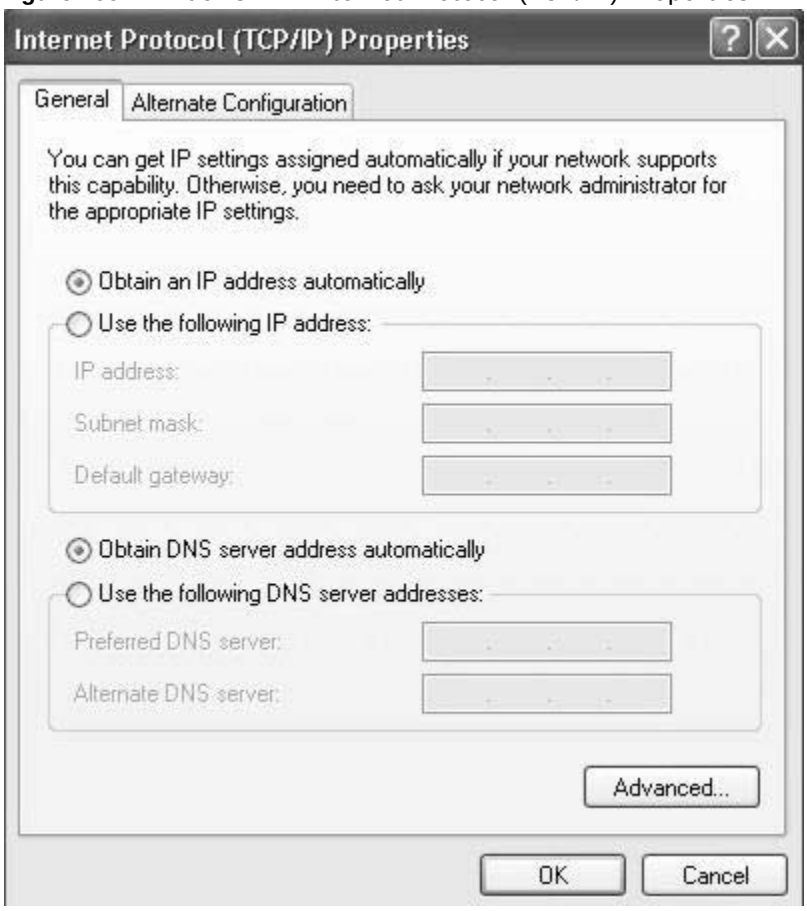
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 165 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 166 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

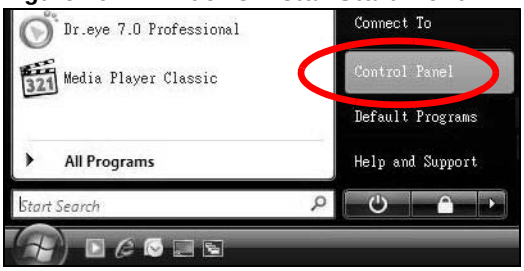
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

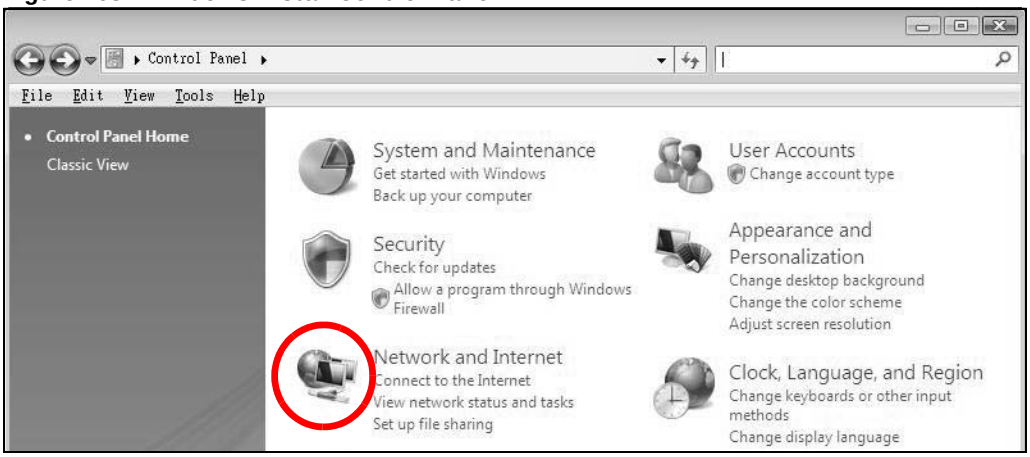
1 Click **Start** > **Control Panel**.

Figure 167 Windows Vista: Start Menu



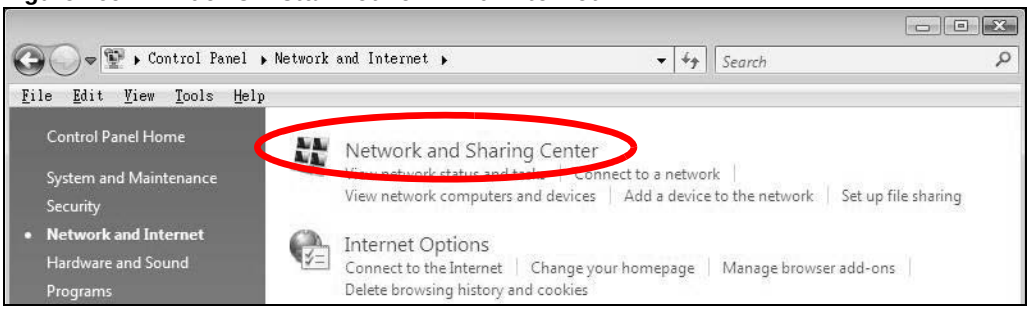
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 168 Windows Vista: Control Panel



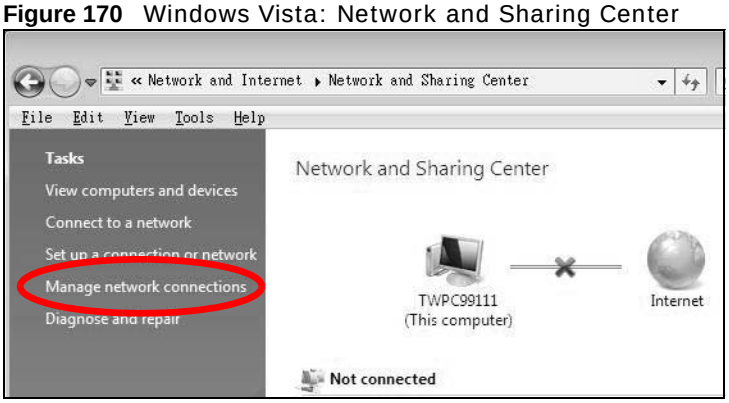
3 Click the **Network and Sharing Center** icon.

Figure 169 Windows Vista: Network And Internet



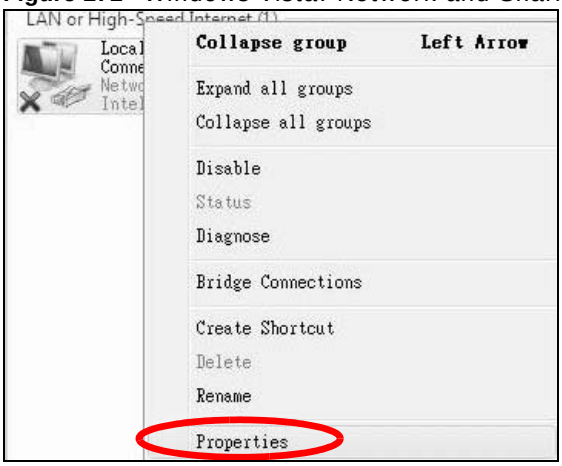
4 Click **Manage network connections**.

Figure 170 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then select **Properties**.

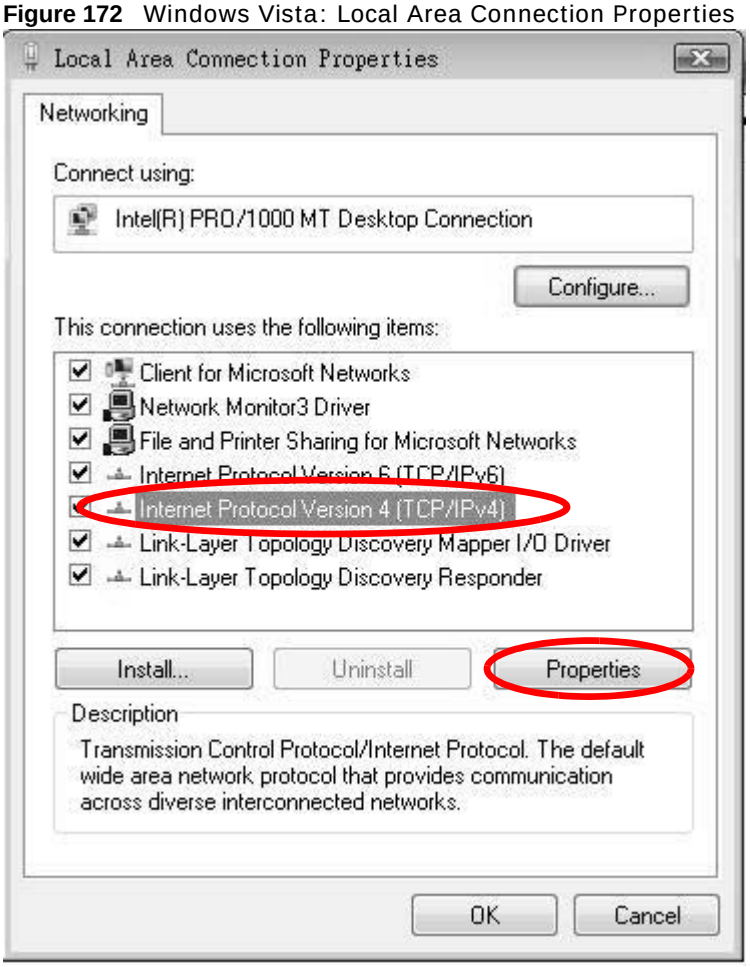
Figure 171 Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

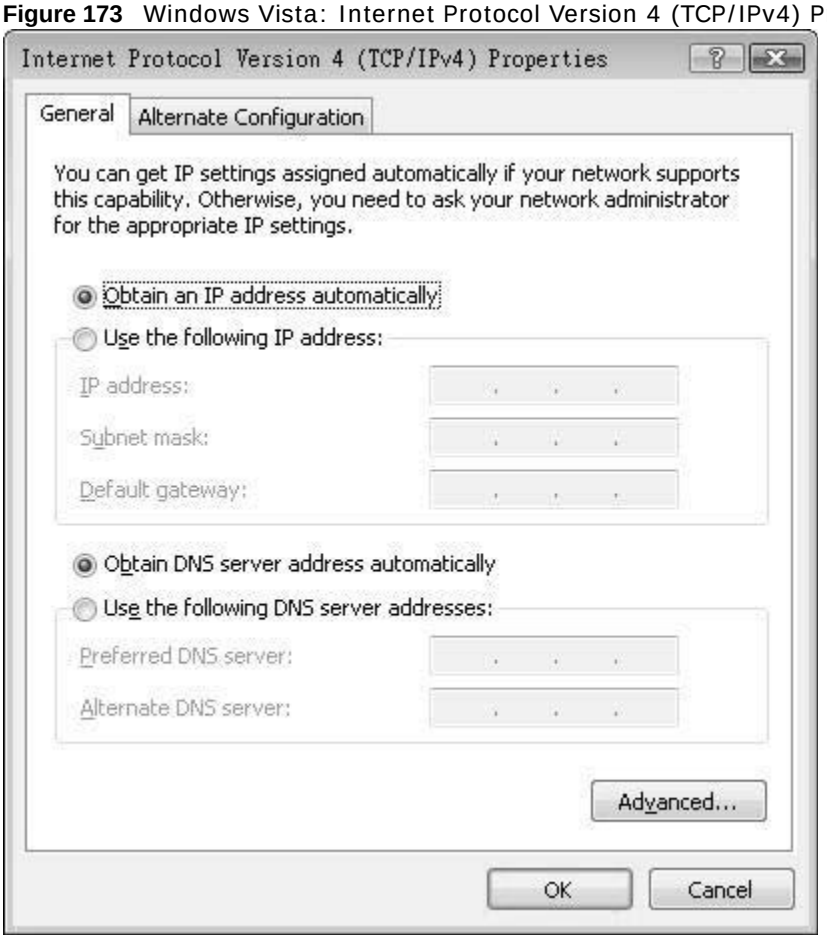
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 172 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 173 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

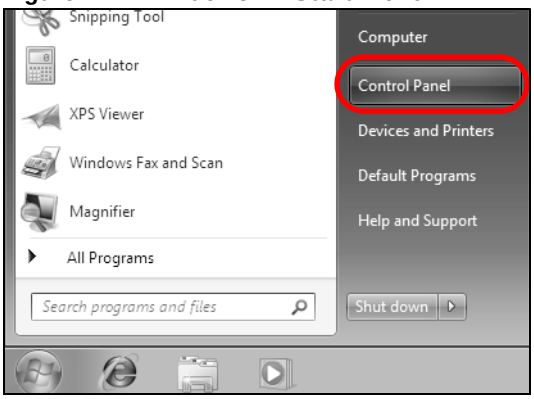
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

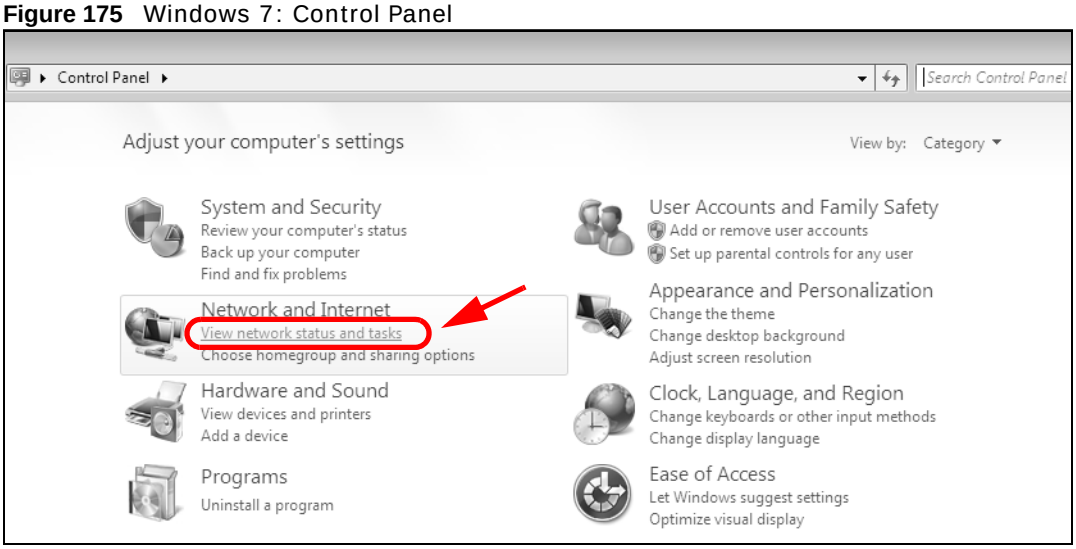
1 Click **Start** > **Control Panel**.

Figure 174 Windows 7: Start Menu



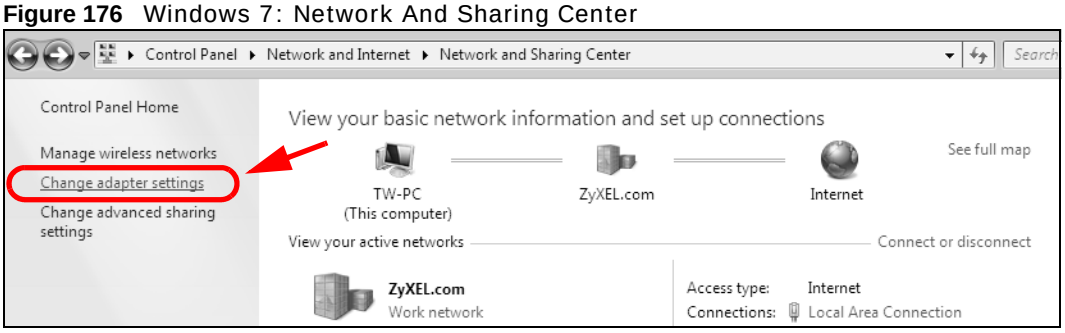
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 175 Windows 7: Control Panel



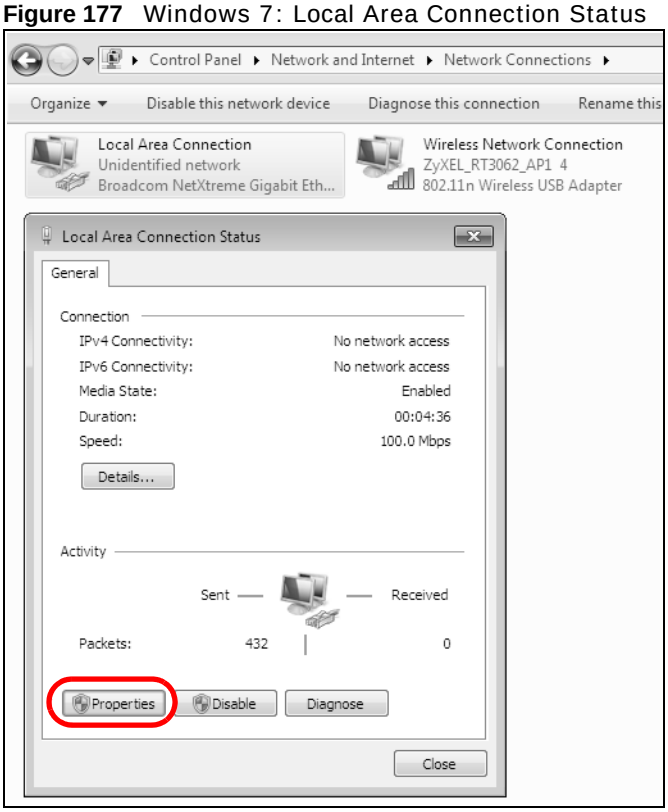
3 Click **Change adapter settings**.

Figure 176 Windows 7: Network And Sharing Center



4 Double click **Local Area Connection** and then select **Properties**.

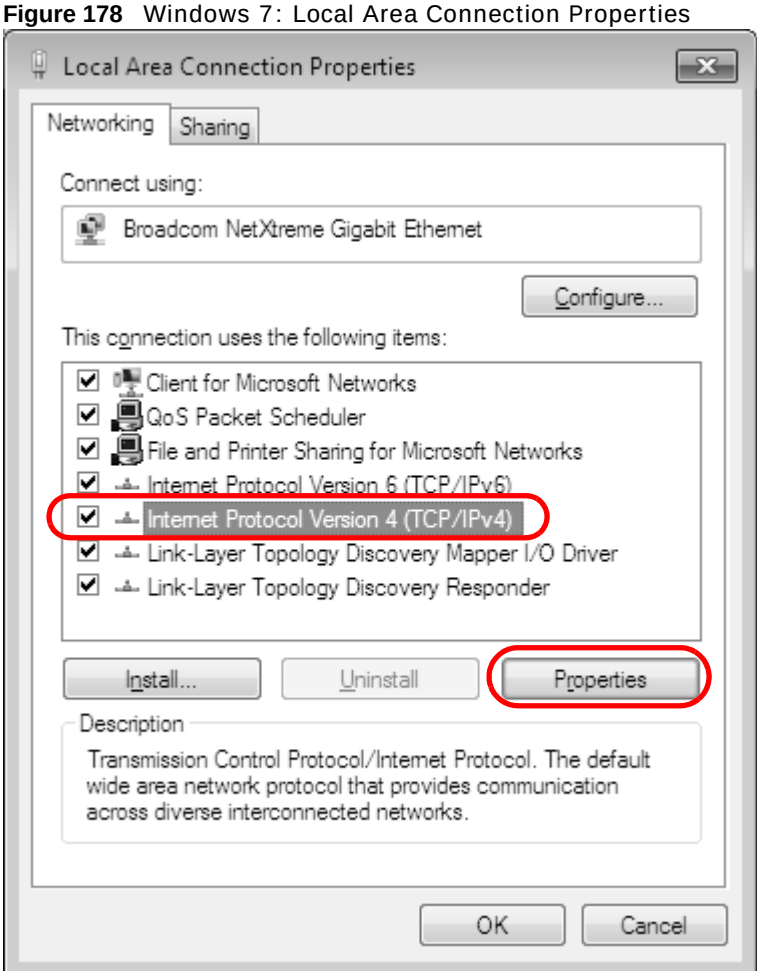
Figure 177 Windows 7: Local Area Connection Status



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

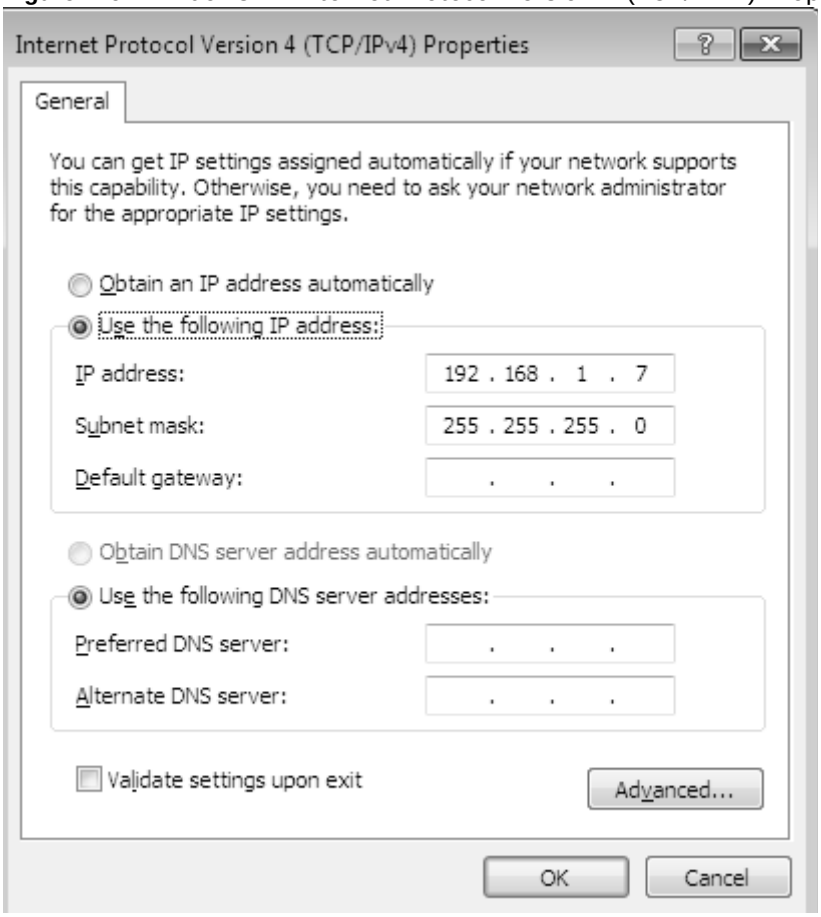
5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 178 Windows 7: Local Area Connection Properties



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 179 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 7
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

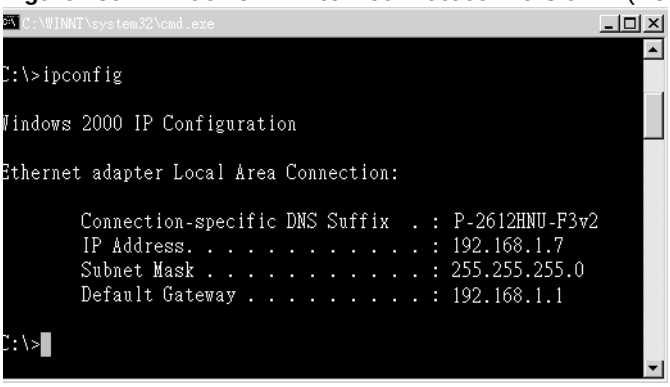
Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

3 The IP settings are displayed as follows.

Figure 180 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties


C:\WINNT\system32\cmd.exe
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : P-2612HNU-F3v2
IP Address. . . . . : 192.168.1.7
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\>

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

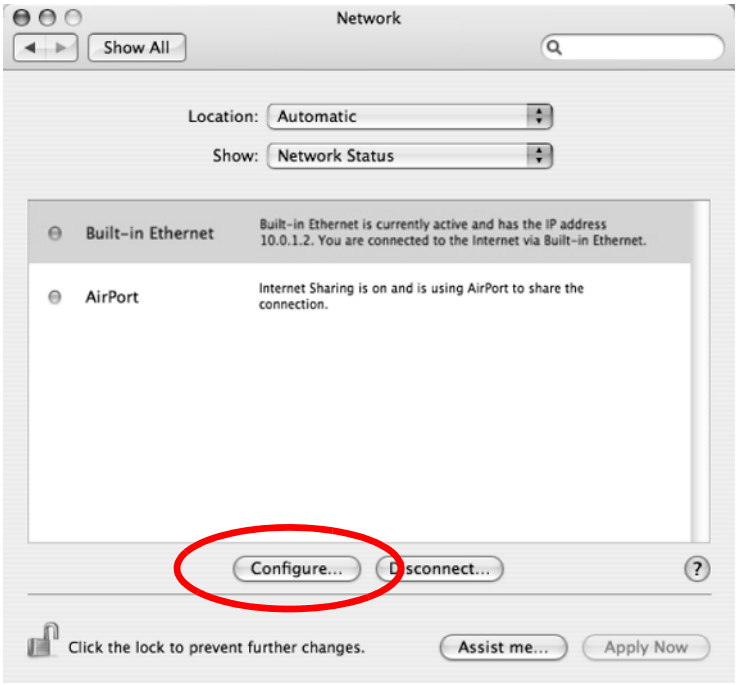
Figure 181 Mac OS X 10.4: Apple Menu

2 In the **System Preferences** window, click the **Network** icon.

Figure 182 Mac OS X 10.4: System Preferences

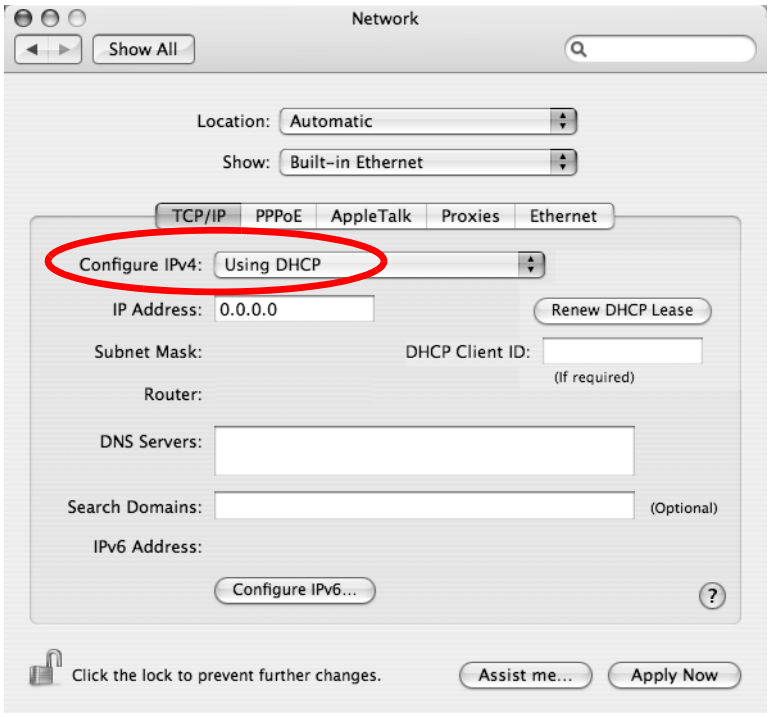
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 183 Mac OS X 10.4: Network Preferences


Network
Show All
Location: Automatic
Show: Network Status
Built-in Ethernet
Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.
AirPort
Internet Sharing is on and is using AirPort to share the connection.
Configure...
Disconnect...
Click the lock to prevent further changes.
Assist me...
Apply Now

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 184 Mac OS X 10.4: Network Preferences > TCP/IP Tab.

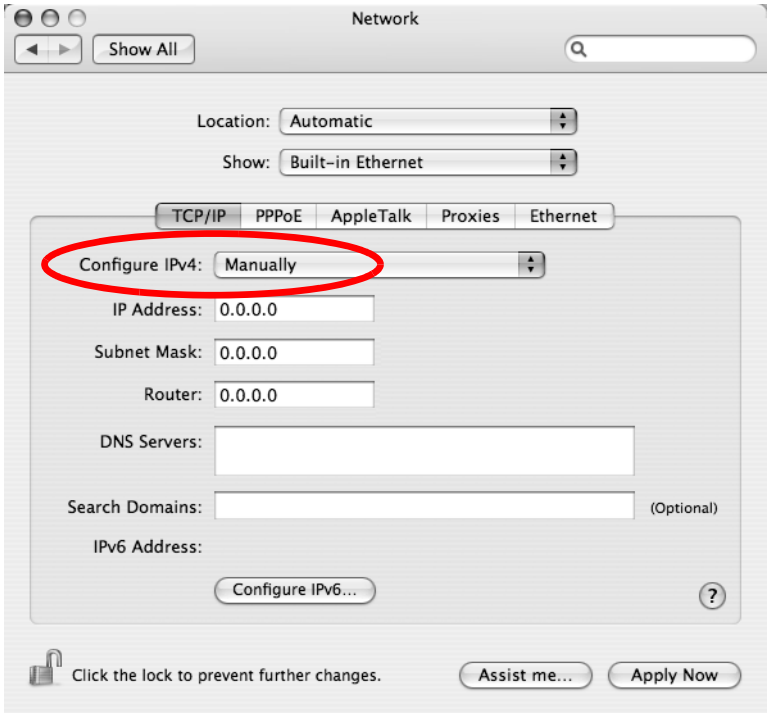


5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.

- In the **Router** field, type the IP address of your device.

Figure 185 Mac OS X 10.4: Network Preferences > Ethernet

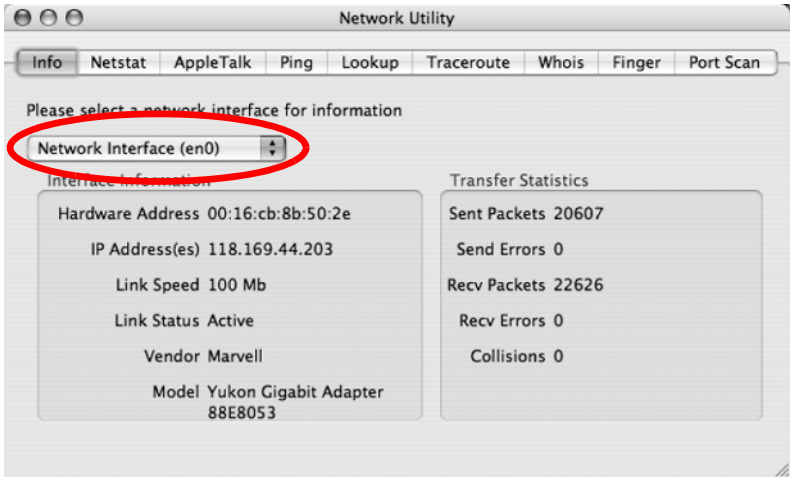


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 186 Mac OS X 10.4: Network Utility

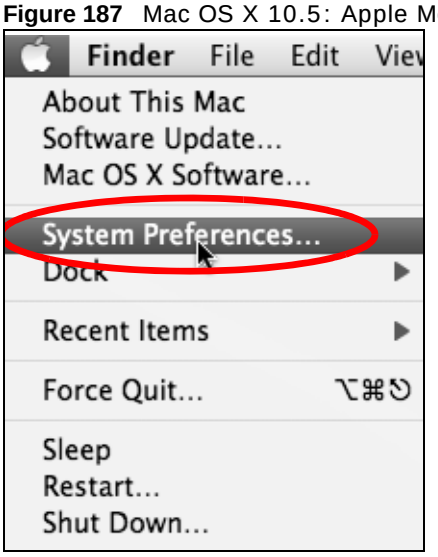


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

1 Click **Apple** > **System Preferences**.

Figure 187 Mac OS X 10.5: Apple Menu

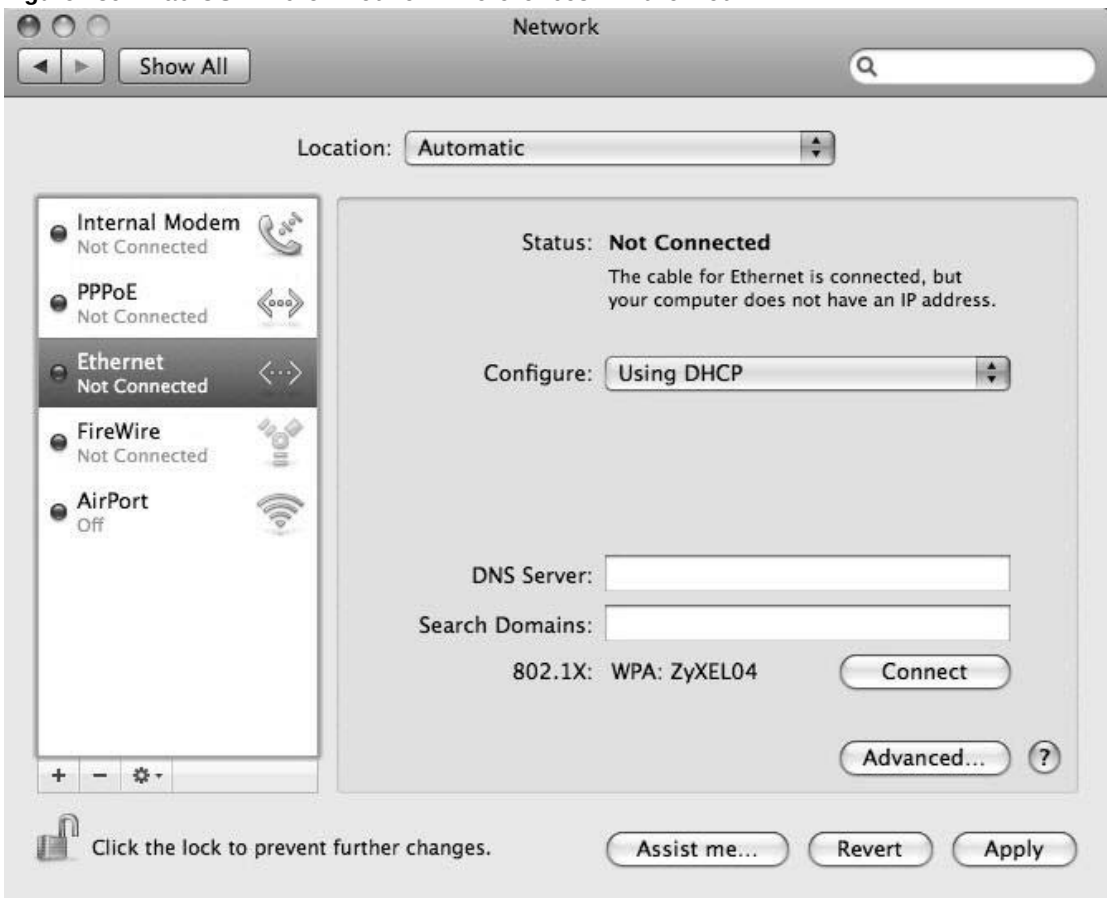


2 In **System Preferences**, click the **Network** icon.

Figure 188 Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 189 Mac OS X 10.5: Network Preferences > Ethernet



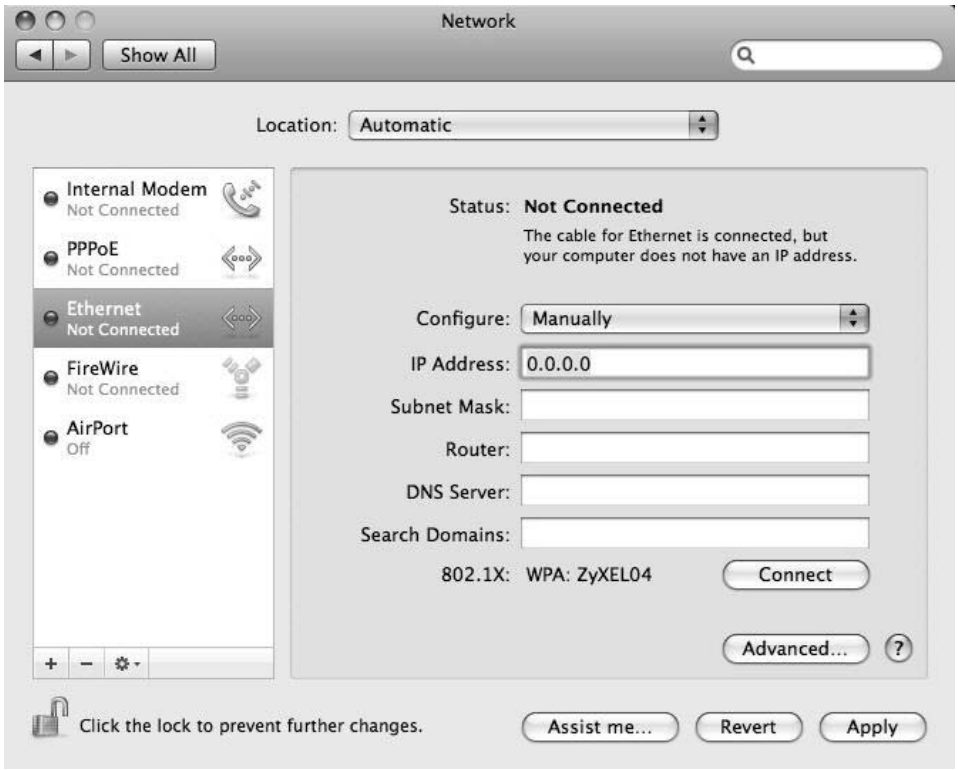
4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your Device.

Figure 190 Mac OS X 10.5: Network Preferences > Ethernet

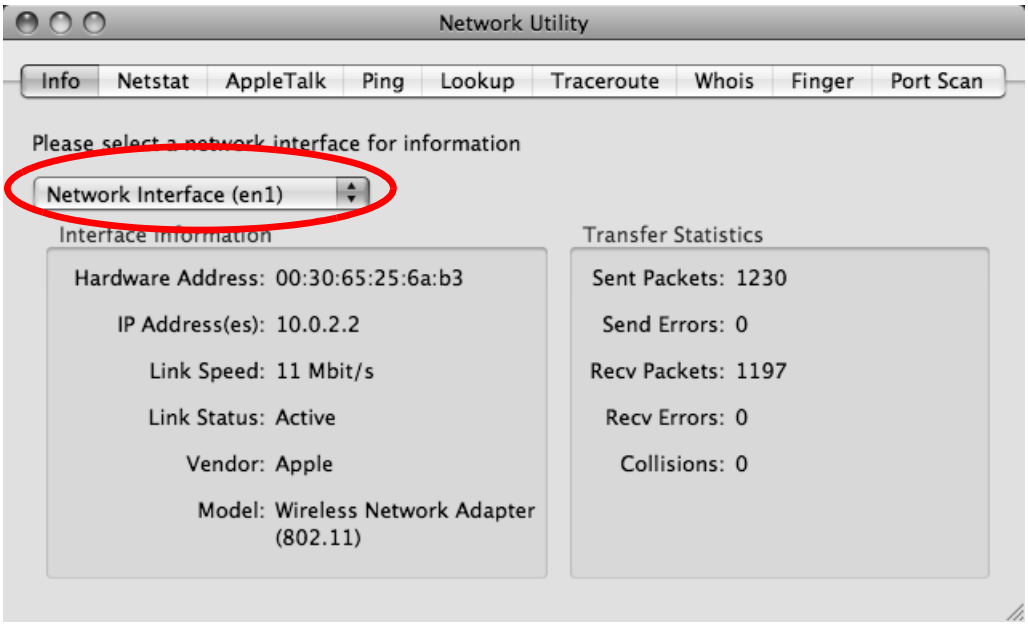


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 191 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

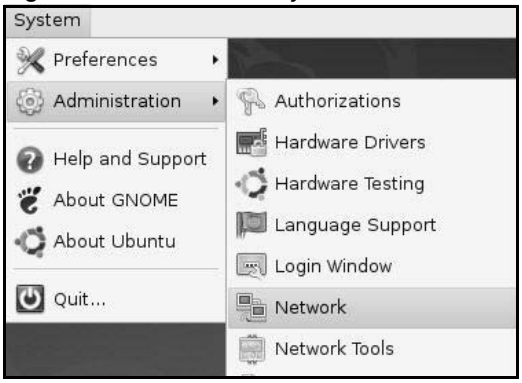
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

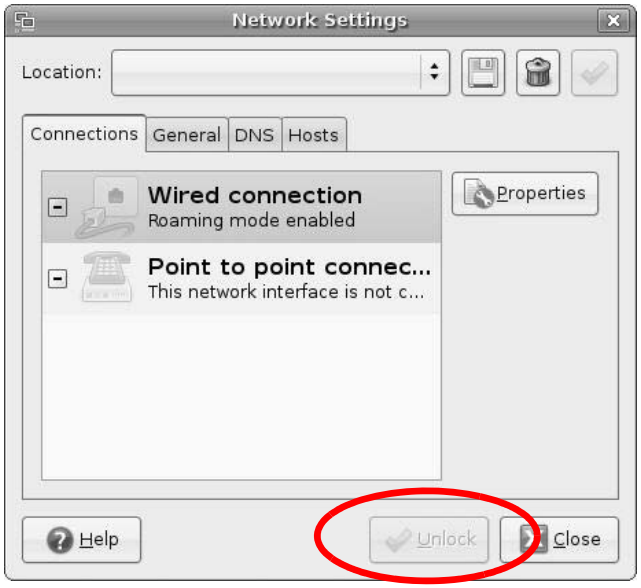
1 Click **System > Administration > Network**.

Figure 192 Ubuntu 8: System > Administration Menu



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 193 Ubuntu 8: Network Settings > Connections



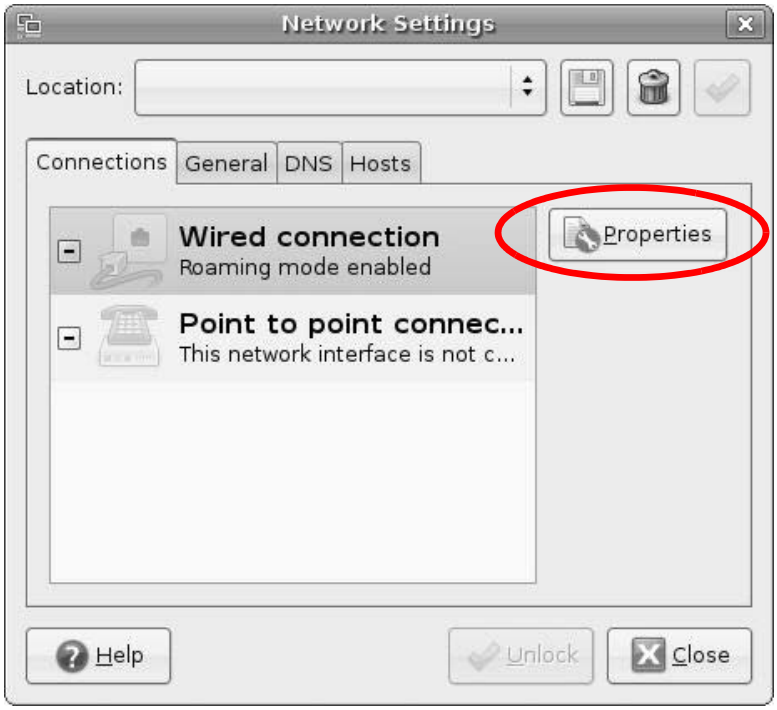
3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 194 Ubuntu 8: Administrator Account Authentication

Authenticate
System policy prevents modifying the configuration
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
C.J.,,,, (chris)
Password for chris:
Details
Cancel
Authenticate

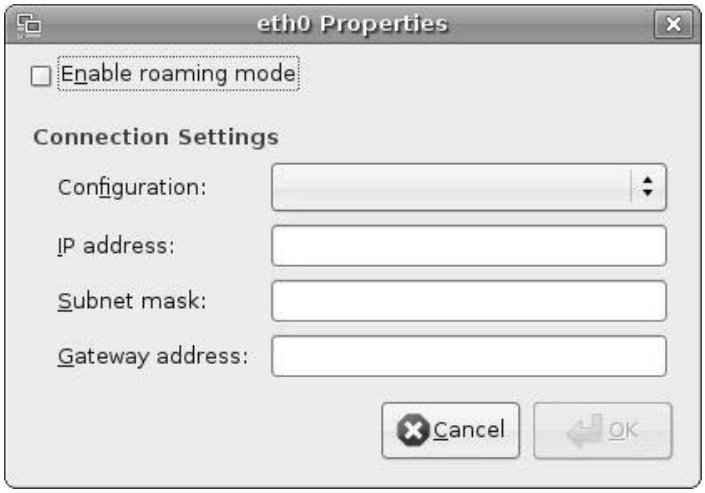
4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 195 Ubuntu 8: Network Settings > Connections



5 The **Properties** dialog box opens.

Figure 196 Ubuntu 8: Network Settings > Properties

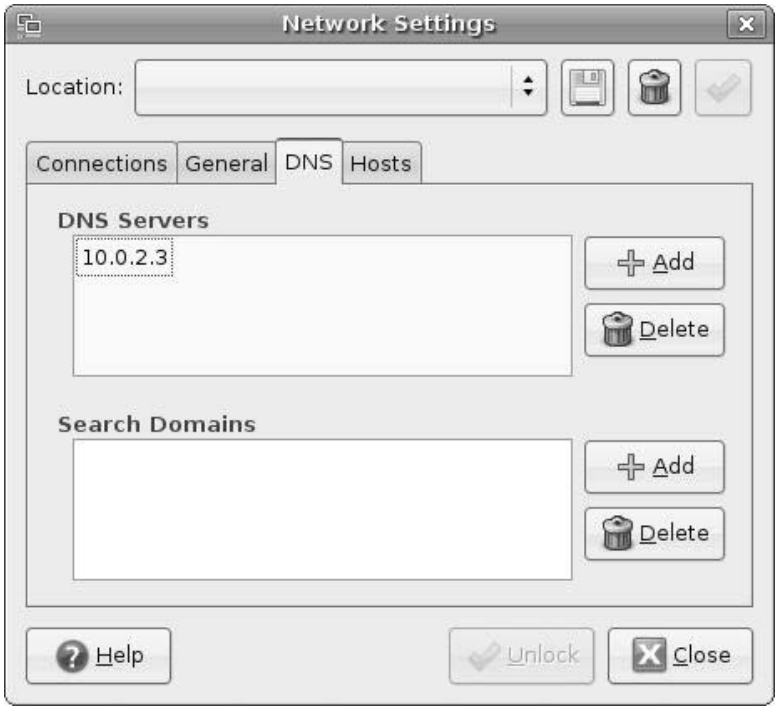


- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 197 Ubuntu 8: Network Settings > DNS

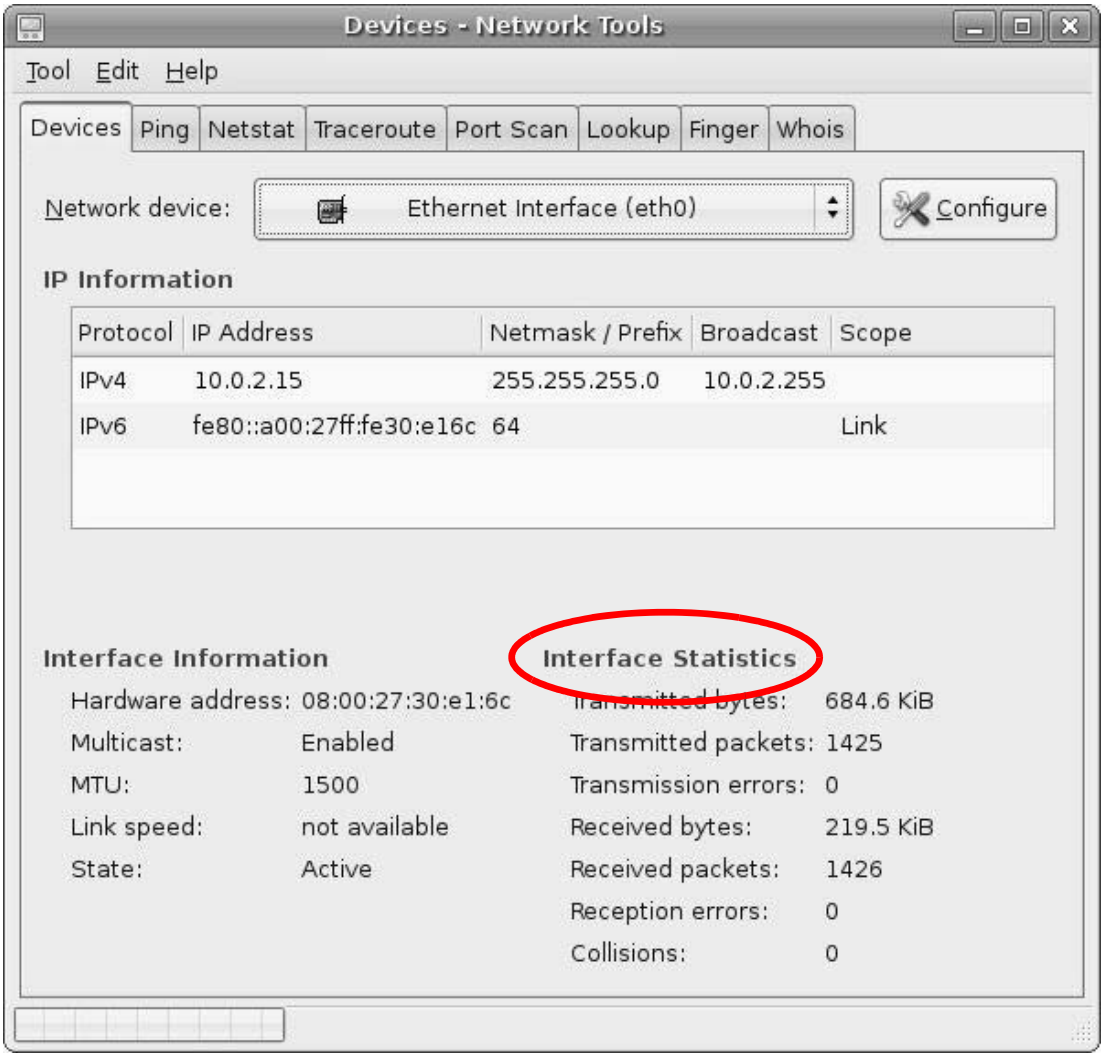


8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 198 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

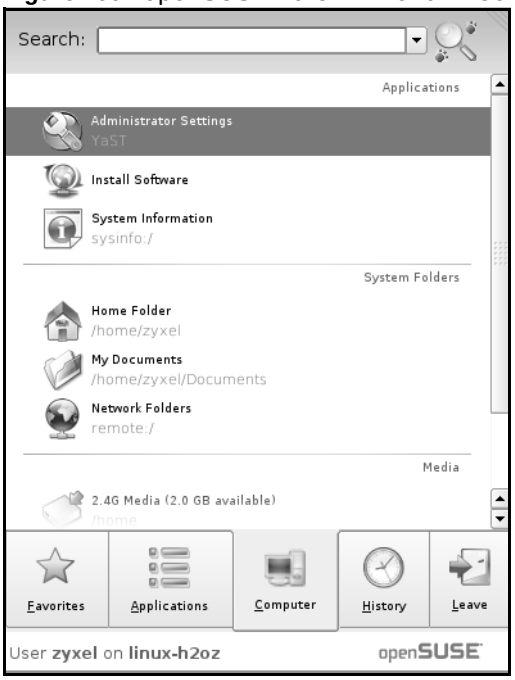
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

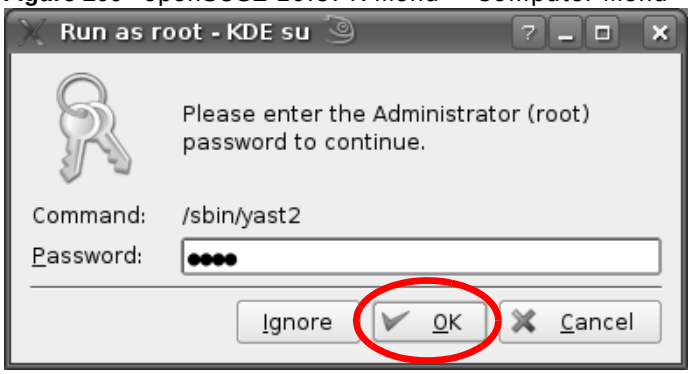
1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 199 openSUSE 10.3: K Menu > Computer Menu



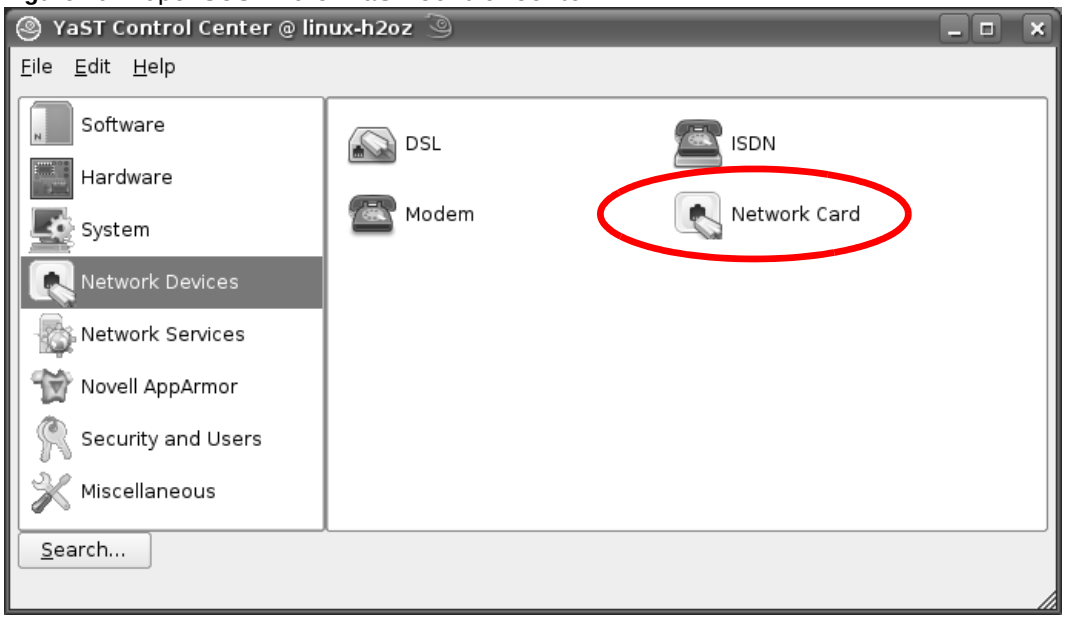
2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 200 openSUSE 10.3: K Menu > Computer Menu



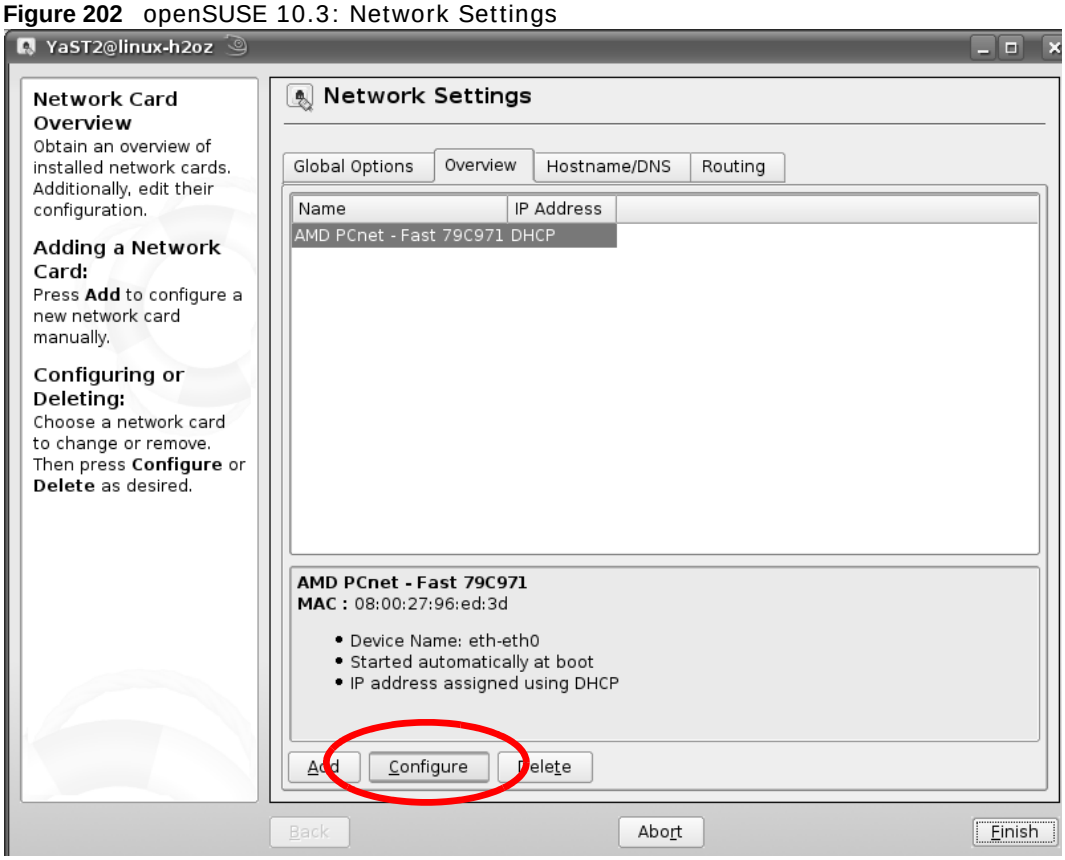
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 201 openSUSE 10.3: YaST Control Center



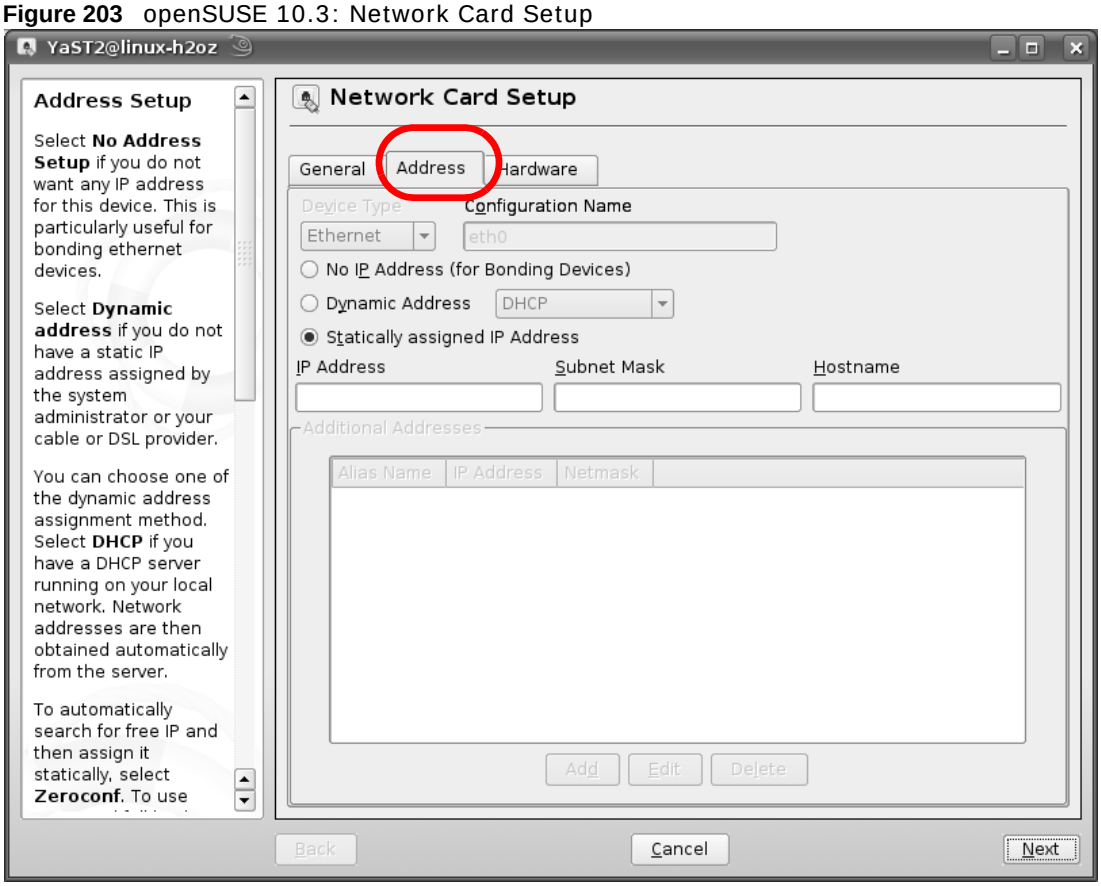
4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 202 openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 203 openSUSE 10.3: Network Card Setup


YaST2@linux-h2oz
Address Setup
Select No Address Setup if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.
Select Dynamic address if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.
You can choose one of the dynamic address assignment method. Select DHCP if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.
To automatically search for free IP and then assign it statically, select Zeroconf. To use
Network Card Setup
General
Address
Hardware
Device Type
Configuration Name
Ethernet
eth0
No IP Address (for Bonding Devices)
Dynamic Address
DHCP
Statically assigned IP Address
IP Address
Subnet Mask
Hostname
Additional Addresses
Alias Name
IP Address
Netmask
Add
Edit
Delete
Back
Cancel
Next

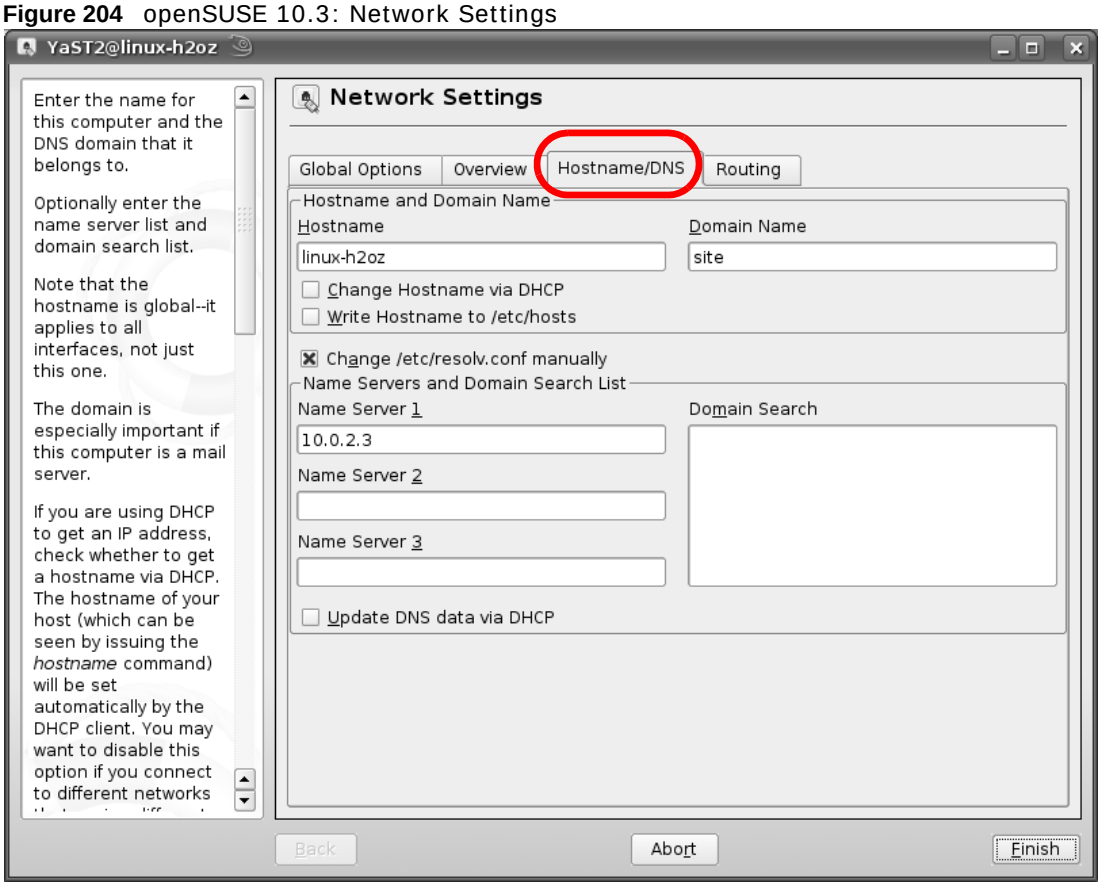
6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 204 openSUSE 10.3: Network Settings

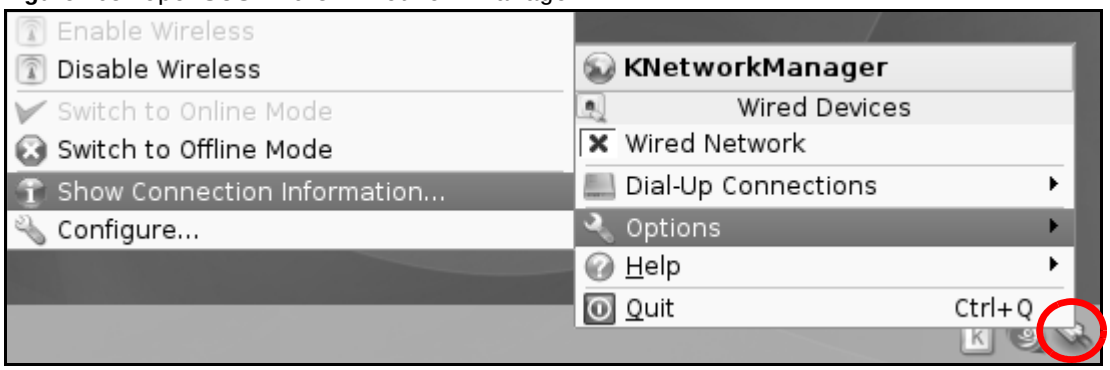

YaST2@linux-h2oz
Enter the name for this computer and the DNS domain that it belongs to.
Optionally enter the name server list and domain search list.
Note that the hostname is global--it applies to all interfaces, not just this one.
The domain is especially important if this computer is a mail server.
If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the hostname command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks
Network Settings
Global Options
Overview
Hostname/DNS
Routing
Hostname and Domain Name
Hostname
linux-h2oz
Domain Name
site
Change Hostname via DHCP
Write Hostname to /etc/hosts
Change /etc/resolv.conf manually
Name Servers and Domain Search List
Name Server 1
10.0.2.3
Domain Search
Name Server 2
Name Server 3
Update DNS data via DHCP
Back
Abort
Finish

9 Click **Finish** to save your settings and close the window.

Verifying Settings

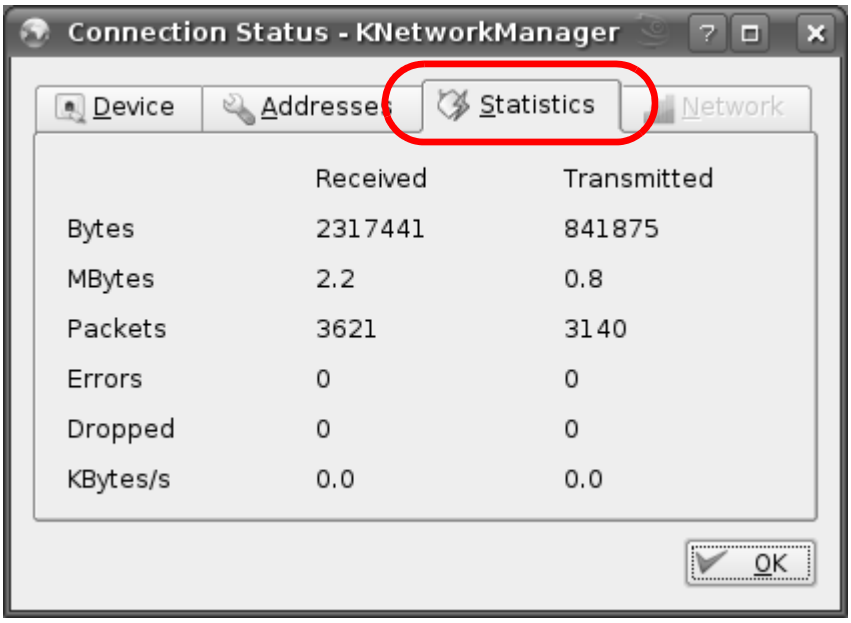
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 205 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 206 openSUSE: Connection Status - KNetwork Manager



C

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

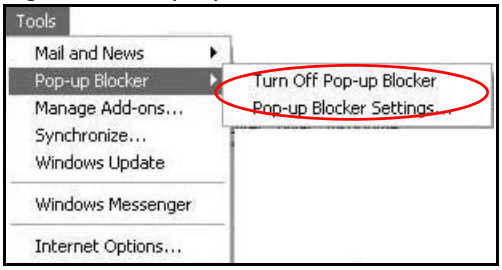
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 207 Pop-up Blocker

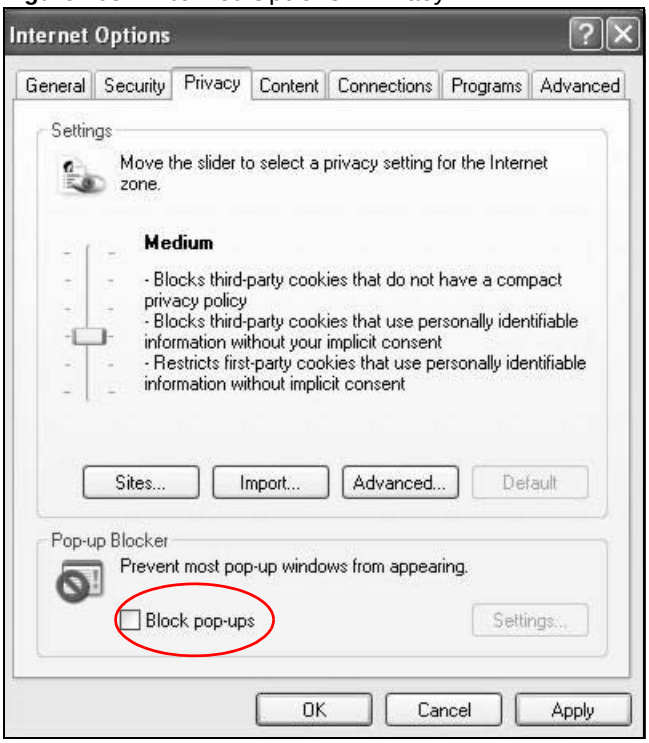


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 208 Internet Options: Privacy



3 Click **Apply** to save this setting.

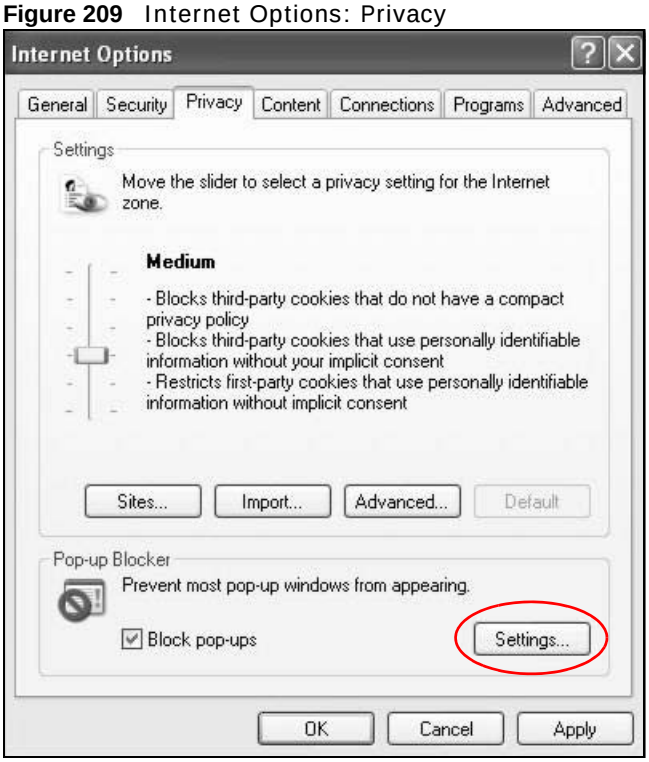
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

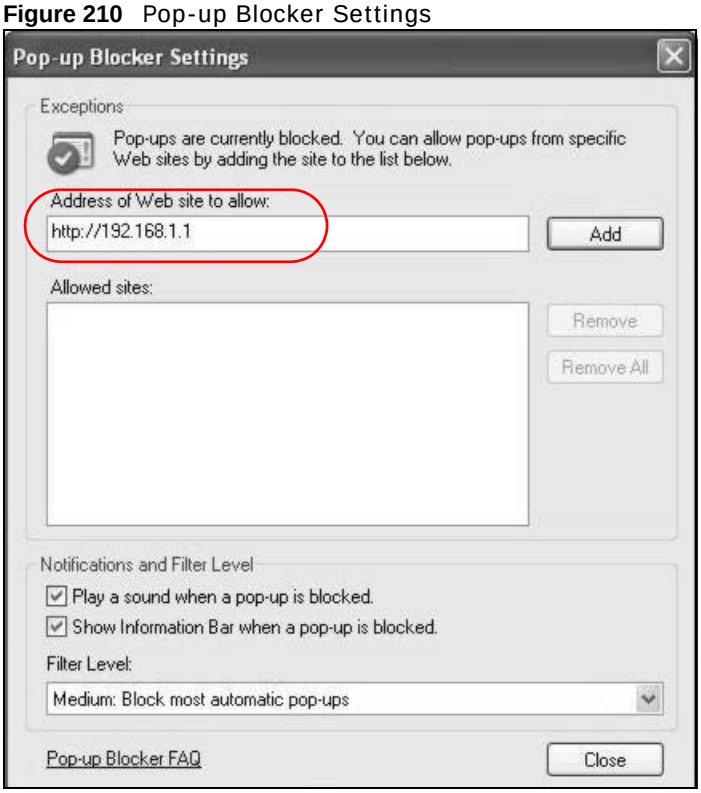
Figure 209 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 210 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

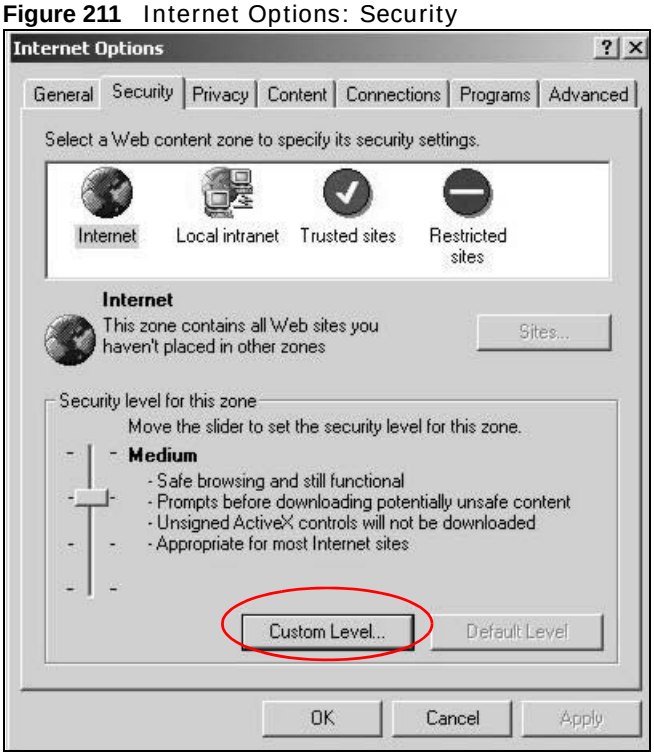
6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 211 Internet Options: Security



2 Click the **Custom Level...** button.

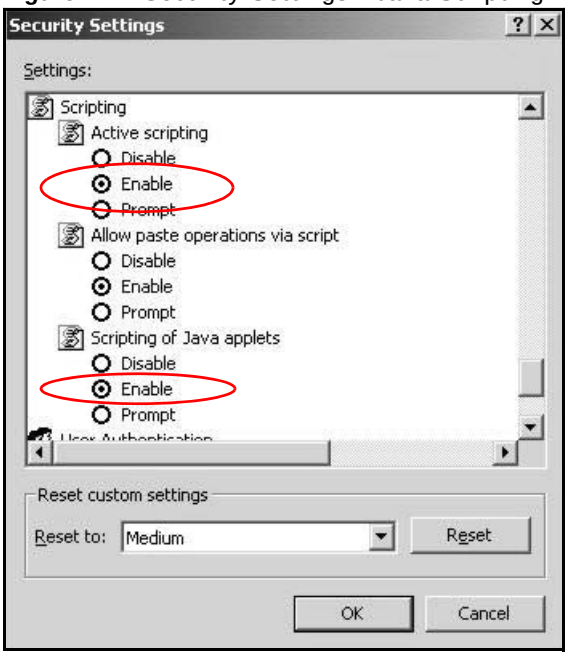
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 212 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

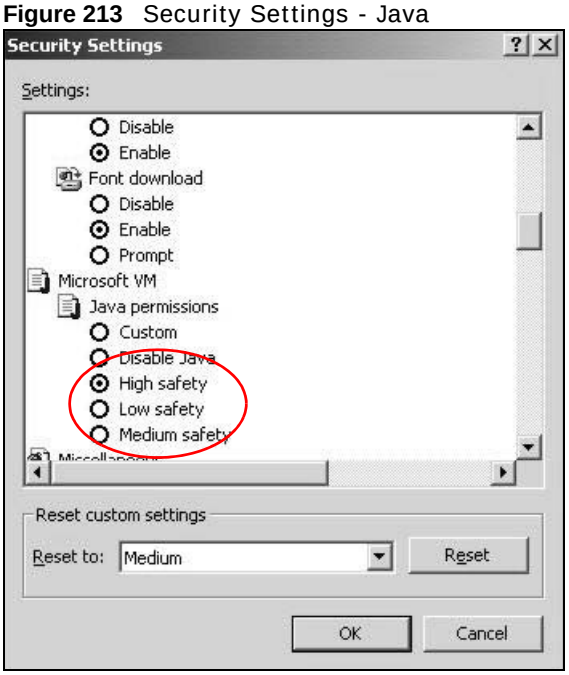
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 213 Security Settings - Java



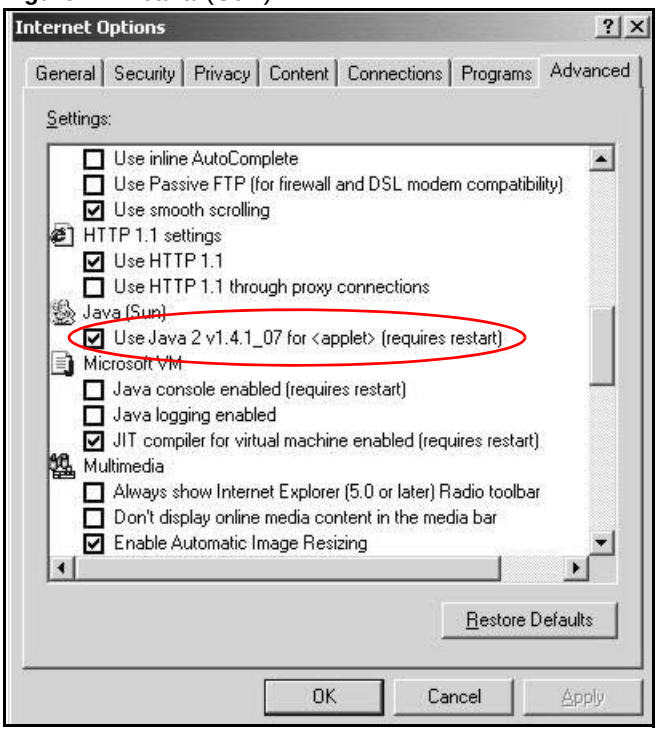
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 214 Java (Sun)

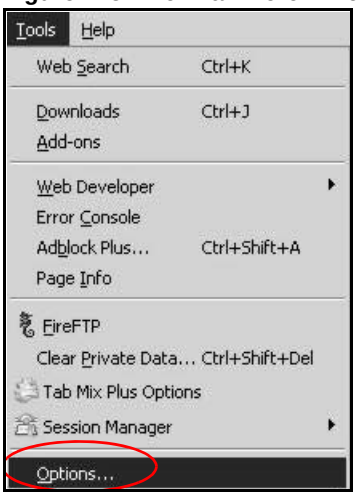


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

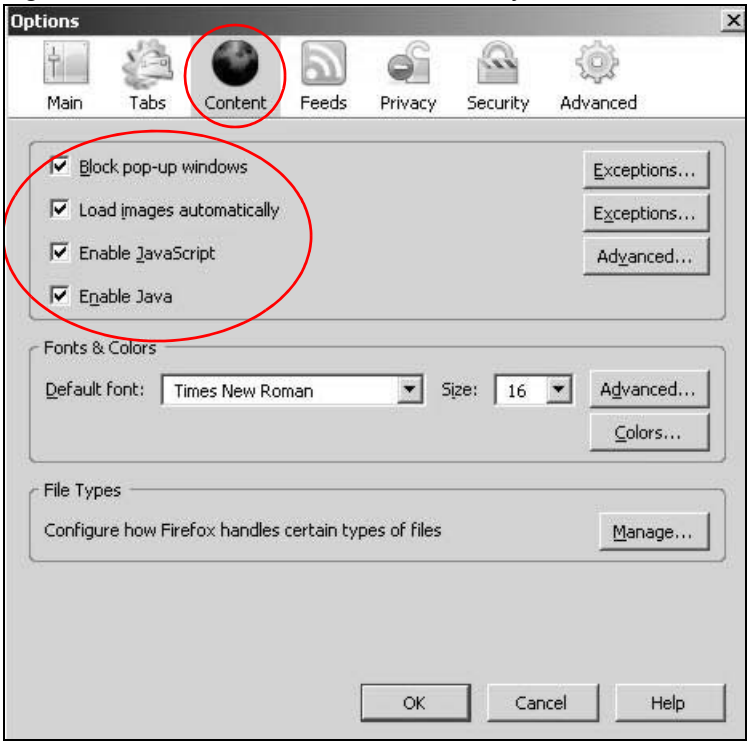
You can enable Java, JavaScript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 215 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 216 Mozilla Firefox Content Security



D

Wireless LANs

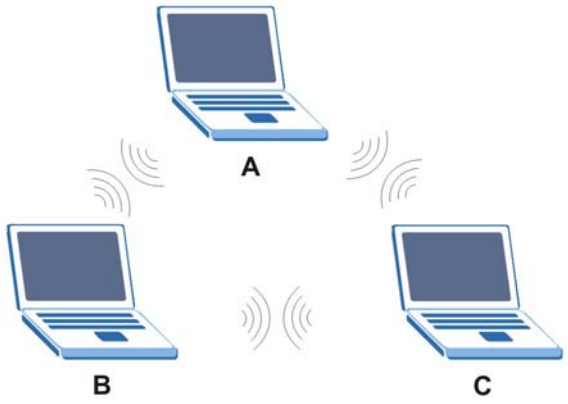
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 217 Peer-to-Peer Communication in an Ad-hoc Network



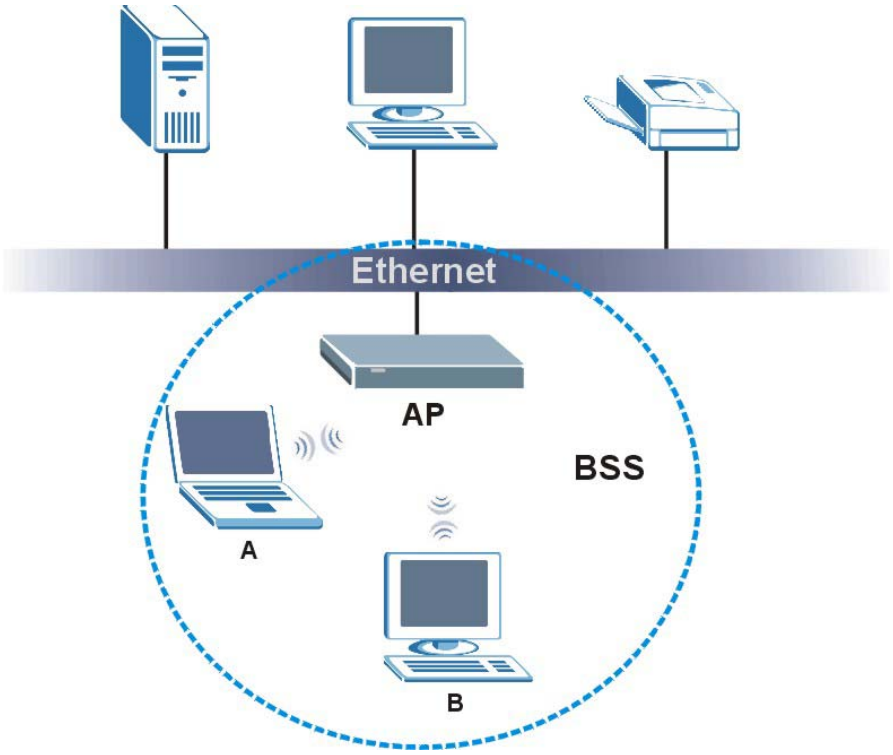
BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is

disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 218 Basic Service Set



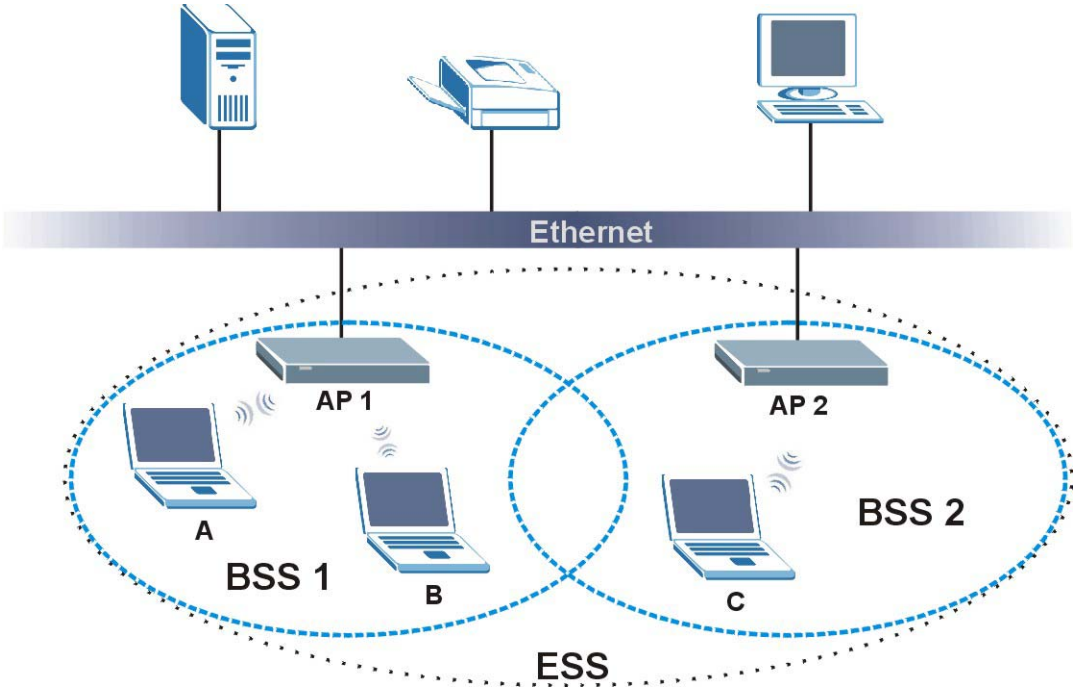
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 219 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

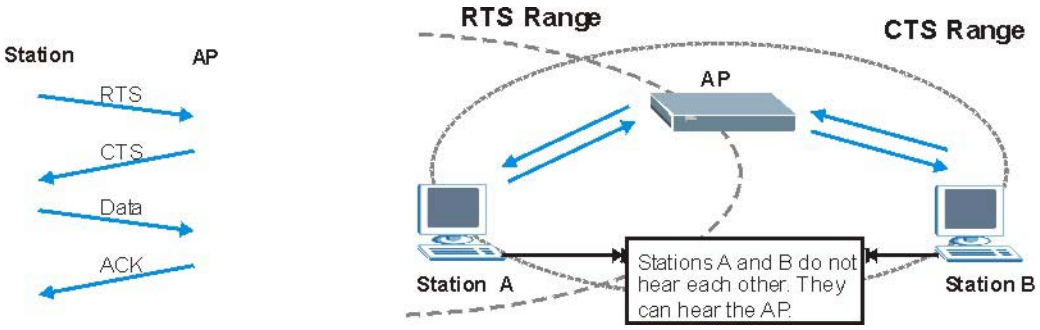
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they

cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 220 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the Device uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 117 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Device.

Table 118 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
	WPA2
Most Secure	

Note: You must enable the same wireless security settings on the Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 119 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm

called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

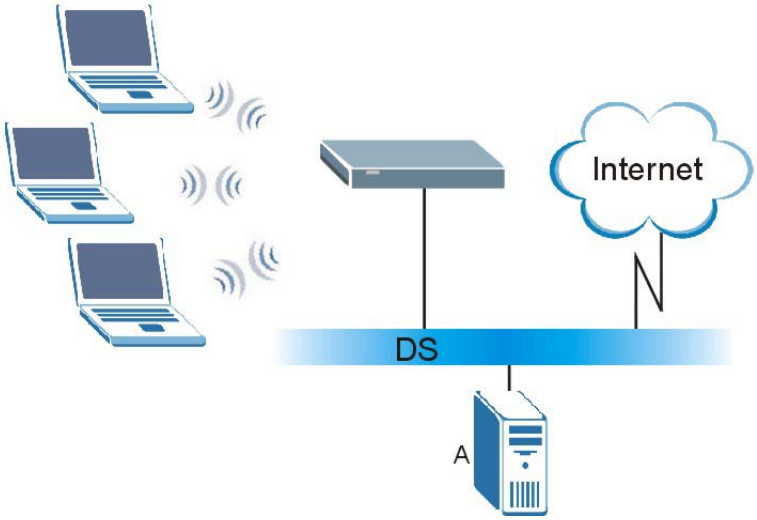
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 221 WPA(2) with RADIUS Application Example



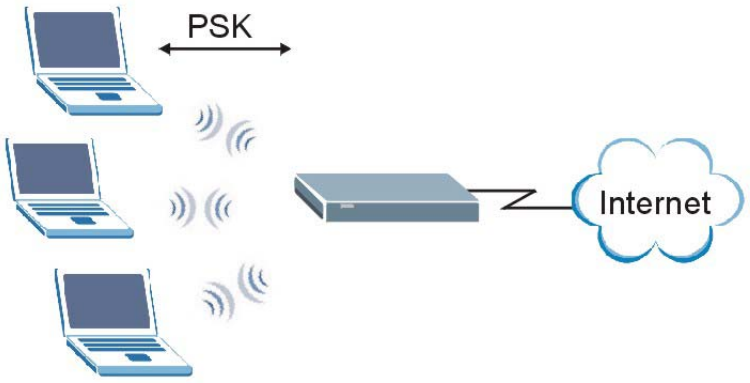
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.
3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 222 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 120 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

WiFi Protected Setup

Your Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Device, see Section 6.4 on page 105).
3. Press the button on one of the devices (it doesn't matter which).
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (you can change it to a new random number by clicking on a button in the configuration interface).

When you use the PIN method, you must enter the enrollee's PIN into the registrar. Then, when WPS is activated on the enrollee, it presents its PIN to the registrar. If the PIN matches, the registrar sends the network and security information to the enrollee, allowing it to join the network.

The advantage of using the PIN method rather than the PBC method is that you can ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in the area. However, you need to log into the configuration interfaces of both devices.

Take the following steps to set up WPS using the PIN method.

1 Decide which device you want to be the registrar (usually the AP) and which you want to be the enrollee (usually the client).

2 Look for the enrollee's WPS PIN; it may be displayed on the device. If you don't see it, log into the enrollee's configuration interface and locate the PIN. Select the PIN connection mode (not PBC connection mode). See the device's User's Guide for how to do this - for the Device, see Section 6.4 on page 105.

3 Log into the configuration utility of the registrar. Select the PIN connection mode (not the PBC connection mode). Locate the place where you can enter the enrollee's PIN (if you are using the Device, see Section 6.4 on page 105). Enter the PIN from the enrollee device.

4 Activate WPS on both devices within two minutes.

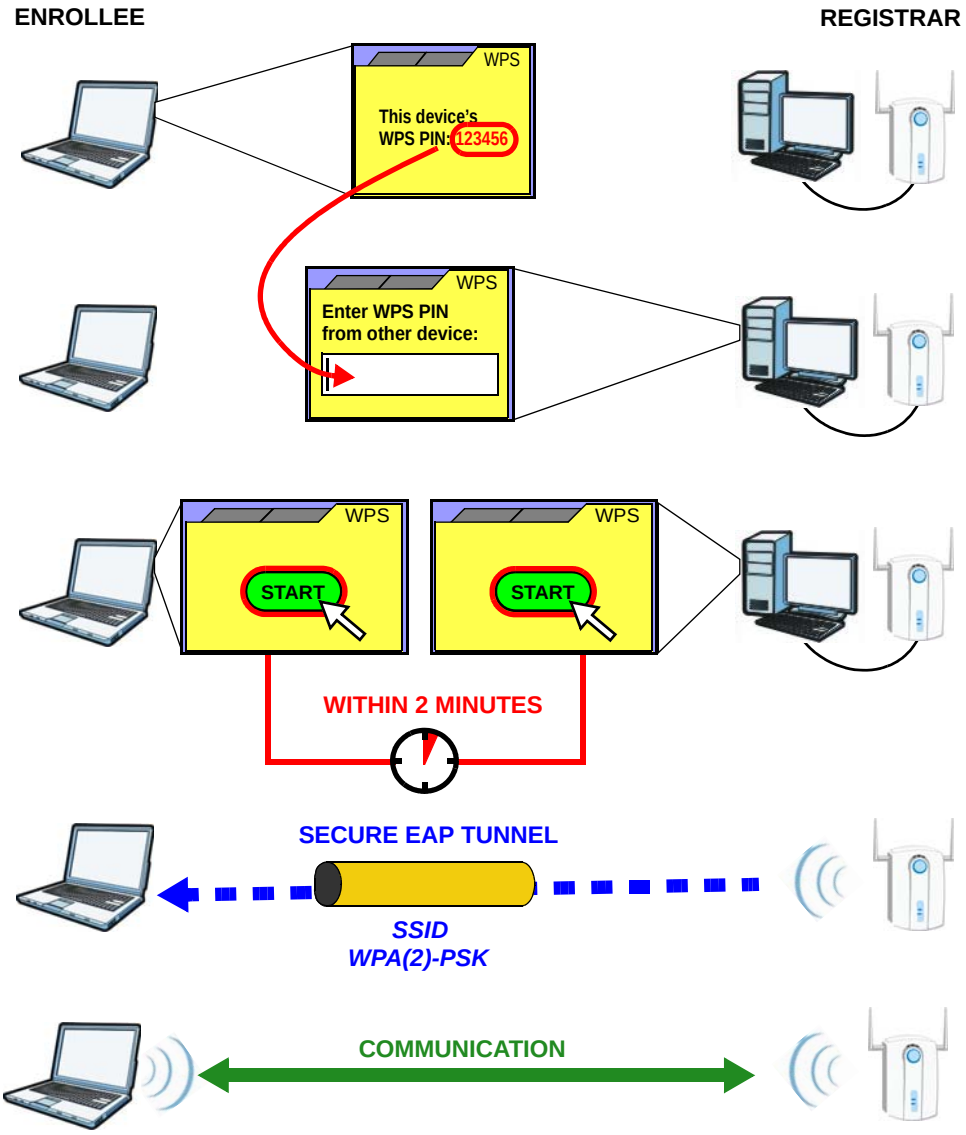
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

5 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 223 Example WPS Process: PIN Method

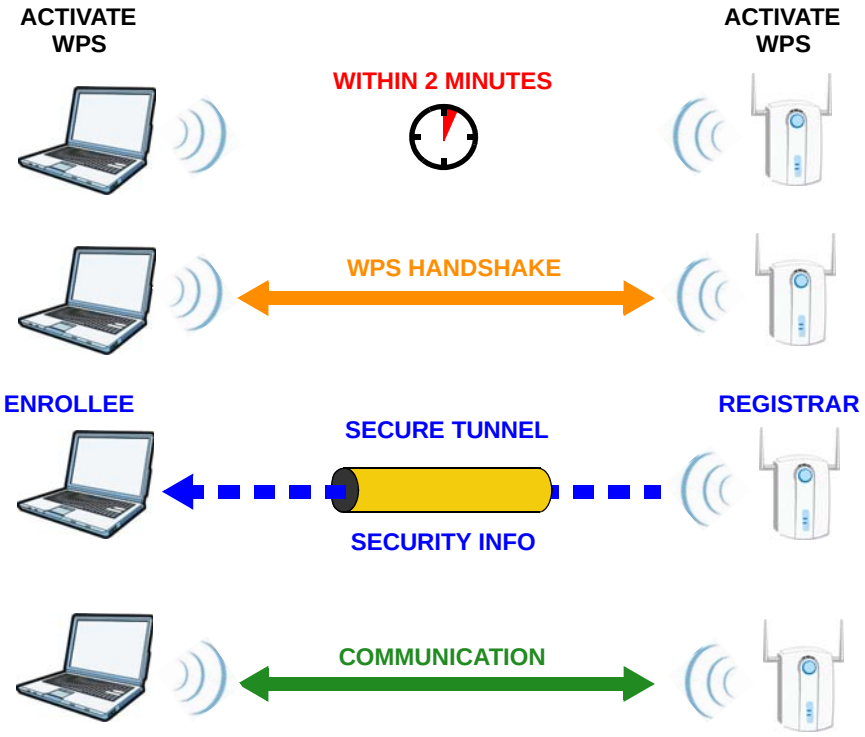


How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 224 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

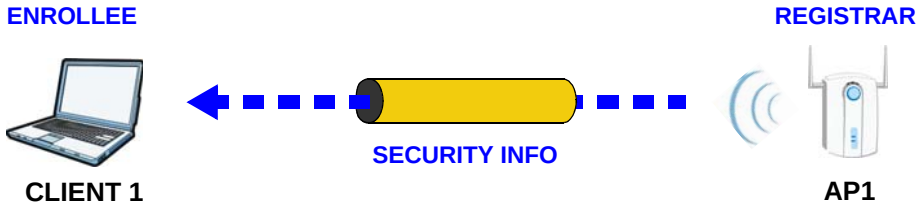
Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1**

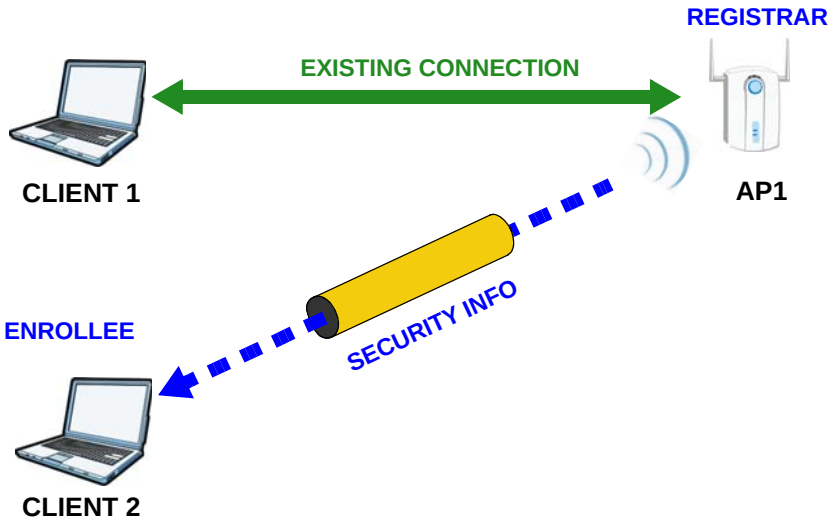
is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 225 WPS: Example Network Step 1



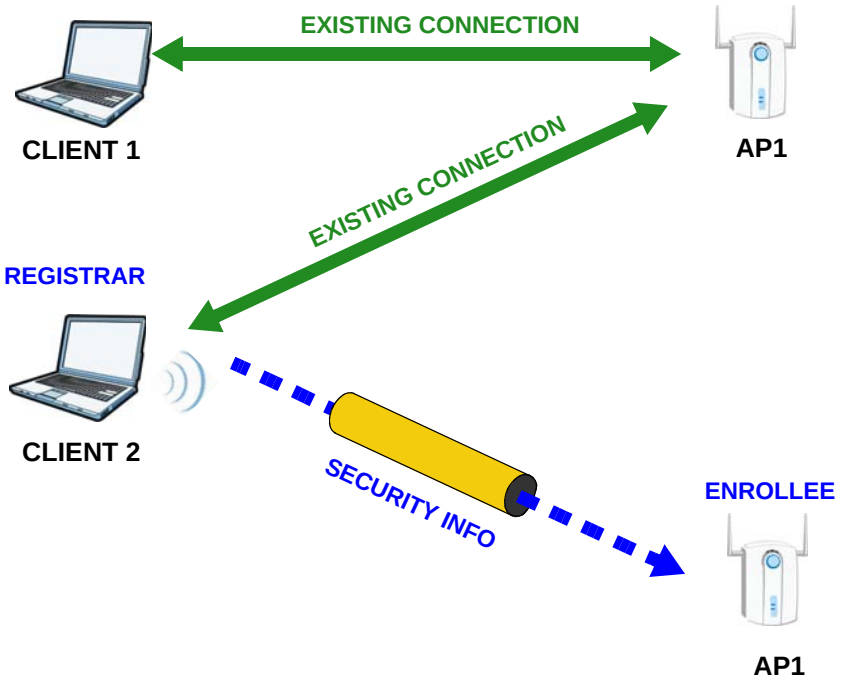
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 226 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 227 WPS: Example Network Step 3



Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 121 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 121 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.

Table 121 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

F

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as “/x” where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 122 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 123 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 124 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

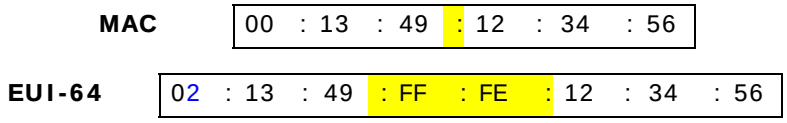
Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the

MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.



Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see Interface ID and EUI-64) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the Device is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [5]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

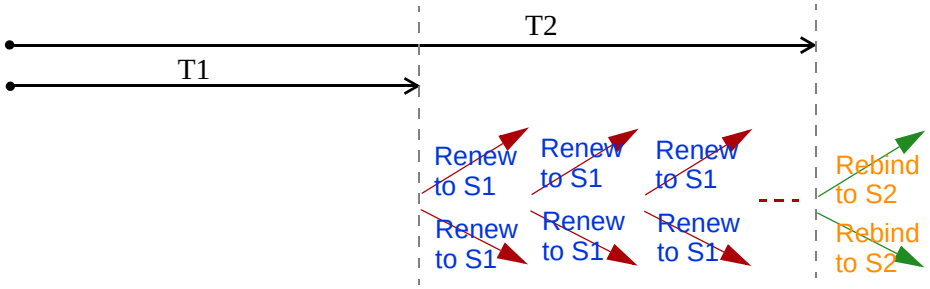
Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the

5. In IPv6, all network interfaces can be associated with several addresses.

IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Device also sends out a neighbor solicitation message. When the Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Device creates an entry in the default router list cache if the router can be used as a default router.

When the Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Device uses the prefix list to determine whether the destination address is on-link

and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This

also displays how to use the ipconfig command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the ipconfig command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

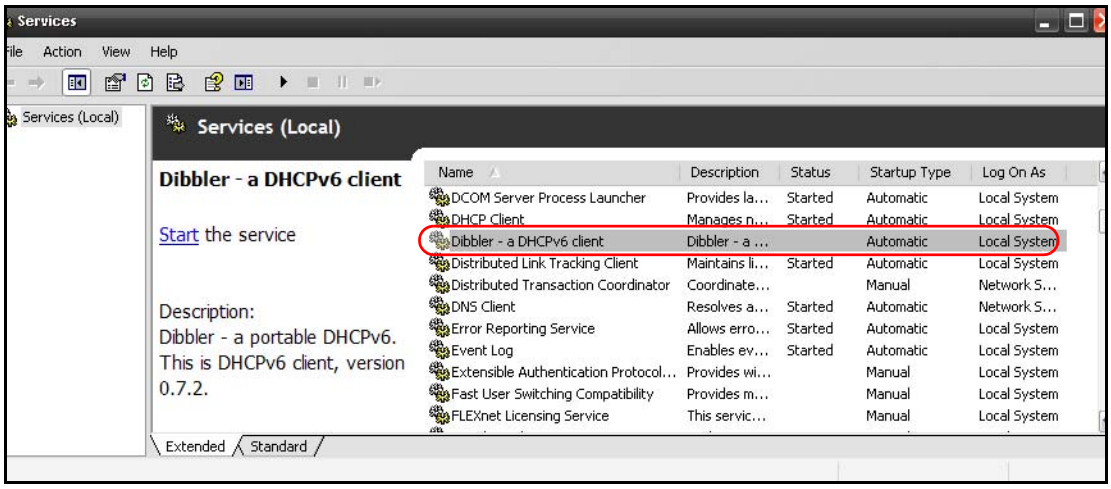
Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

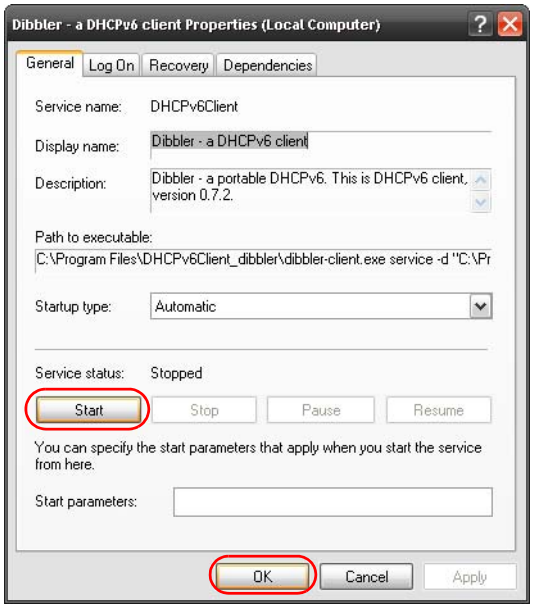
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1. Install Dibbler and select the DHCPv6 client option on your computer.
2. After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.
3. Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



5 Click **Start** and then **OK**.



6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

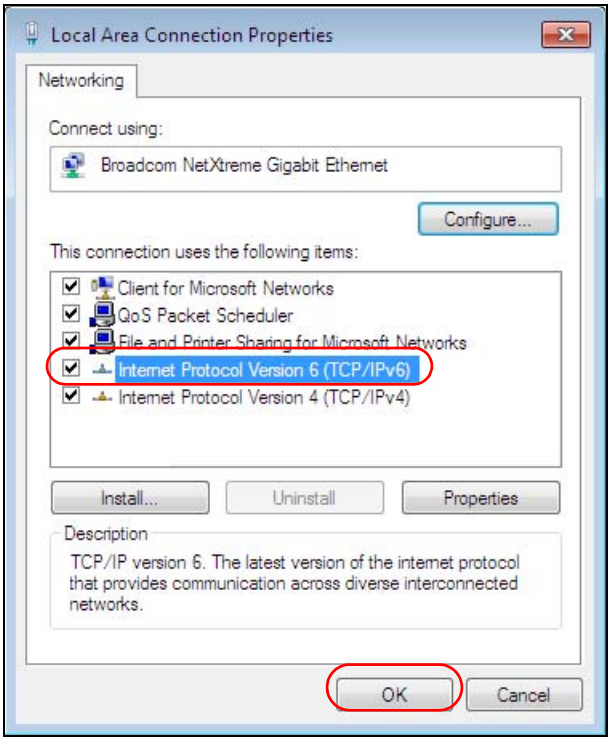
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the ipconfig command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

G

Legal Information

Copyright

Copyright © 2012 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the Device is subject to the terms and conditions of any related service providers. Use with products that have NAT, and/or 3G.

Do not use the Device for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws, and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature. Use for products that have a download service.

Make sure all data and programs on the Device are also stored elsewhere. ZyXEL is not responsible for any loss of or damage to any data, programs, or storage media resulting from the use, misuse, or disuse of this or any other ZyXEL product. Use for storage/backup devices.

Trademarks

This item incorporates copy protection technology that is protected by U.S. patents and other intellectual property rights of Rovi Corporation. Reverse engineering and disassembly are prohibited. Use for STBs that need Rovi certification.

Certifications (Class B)

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, 802.11g or 802.11n(20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n(40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

注意 !

依據 低功率電波輻射性電機管理辦法
第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- This product is for indoor use only (utilisation intérieure exclusivement).
- The RJ-45 jacks are not used for telephone line connection.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

A

ACK message 237
ACL rule 182
activation
  firewalls 178
  media server 130
  SIP ALG 168
  SSID 104
  wireless LAN
    scheduling 108
adding a printer example 55
administrator password 23
Advanced Encryption Standard, see AES
AES 341
AH 211
algorithms 211
alternative subnet mask notation 286
antenna
  directional 345
  gain 345
  omni-directional 345
AP (Access Point) 335
applications
  Internet access 17
  media server 130
    activation 130
    iTunes server 130
  VoIP 18
authentication 110, 111
  RADIUS server 111
automatic logout 24

B

backup
  configuration 267
bandwidth management 149
Basic Service Set, see BSS
blinking LEDs 20
Broadband 81
broadcast 92
BSS 113, 333
  example 113
BYE request 237

C

CA 191, 340
call hold 240
call rule 232
call service mode 239
call transfer 241
call waiting 240
Canonical Format Indicator See CFI
certificate
  factory default 194
Certificate Authority, see CA
certificates 191
  CA 191
  replacing 194
  storage space 194
  thumbprint algorithms 193
  thumbprints 193
  trusted CAs 195
  verifying fingerprints 193
Certification Authority, see CA
certifications 369
  notices 371
  viewing 371
CFI 92
channel 335
  interference 335
channel scan 98
channel, wireless LAN 96
Class of Service 238
Class of Service, see CoS
client list 125

client-server protocol 234
comfort noise generation 222
configuration 132
  backup 267
  firewalls 178
  reset 269
  restoring 268
copyright 369
CoS 160, 238
CTS (Clear to Send) 336
CTS threshold 110

D

data fragment threshold 110
default LAN IP address 23
default server address 165
Denials of Service, see DoS
DH 217
DHCP 78, 122, 132, 133
DHCPv6 83
diagnostic 271
differentiated services 238
Differentiated Services, see DiffServ
Diffie-Hellman key groups 217
DiffServ (Differentiated Services) 238
  code points 238
  marking rule 160, 238
disclaimer 369
DLNA 130
DMZ 165
DNS 122, 171
DNS Server
  for VPN host 215
DNS server address assignment 93
documentation
  related 2
domain name system, see DNS
Domain Name System. See DNS.
DoS 178
DS (Differentiated Services) 160
DS field 160, 238
DSCP 160, 238
DTMF 237
Dual-Tone MultiFrequency, see DTMF
DUID 83
Dynamic Host Configuration Protocol, see DHCP
dynamic secure gateway address 202
dynamic WEP key exchange 340

E

EAP Authentication 339
echo cancellation 222
Encapsulation 91
  MER 91
  PPP over Ethernet 91
encapsulation 82, 213
encryption 112, 341
ESP 211
ESS 334
Europe type call service mode 239
Extended Service Set IDentification 98, 105
Extended Service Set, see ESS

F

FCC interference statement 369
File Sharing 127
filters
  MAC address 111
firewalls 177
  add protocols 179
  configuration 178
  DoS 178
  security 184
firmware 265
flash key 239
flashing 239
fragmentation threshold 110, 336
FTP 162

G

G.168 222
Guide
  Quick Start 2

H

hidden node 335
host 253
host name 77

I

IANA 133, 290
IBSS 333
ID type and content 216
IEEE 802.11g 337
IEEE 802.1Q 92
IEEE 802.1Q VLAN 239
IGMP 92
  version 92
IKE phases 214
importing trusted CAs 195
Independent Basic Service Set, see IBSS
initialization vector (IV) 342
inside header 213
install UPnP 136
  Windows Me 136
  Windows XP 137
interface group 175
Internet Assigned Numbers Authority
  See IANA
Internet Assigned Numbers Authority, see IANA
Internet Key Exchange 214
Internet Protocol Security, see IPSec
Internet Protocol version 6 83
Internet Protocol version 6, see IPv6
Internet Service Provider, see ISP
IP address 78, 133
  default 23
  WAN 82
IP Address Assignment 91
IP pool 125
IP pool setup 132
IPSec 201
  algorithms 211
  architecture 211
  NAT 211
  see also VPN
IPv6 83, 357
  addressing 83, 357
  DHCP 83
  EUI-64 359
  global address 358
  interface ID 359
  link-local address 358
  Neighbor Discovery Protocol 357
  ping 357
  prefix 83, 357
  prefix delegation 84
  prefix length 83, 357
  stateless autoconfiguration 360
  unspecified address 358
ISP 82
iTunes server 130
ITU-T 222

L

LAN 121
  and USB printer 131
  client list 125
  MAC address 126
LAN TCP/IP 133
limitations
  wireless LAN 112
  WPS 118
listening port 225
Local Area Network, see LAN
login
  passwords 23
logout 24
  automatic 24
logs 243, 263

M

MAC 77, 185
MAC address 126
  filter 111
MAC address filtering 185
MAC filter 185
managing the device
  good habits 20
  using FTP. See FTP.
Media access control 185
Media Access Control, see MAC Address
media server 130
  activation 130
  iTunes server 130
Message Integrity Check, see MIC
MIC 341
model name 77
MTU (Multi-Tenant Unit) 92
multicast 92
multimedia 233
my IP address 202

N

NAT 133, 162, 290
  definitions 168
  how it works 169
  IPSec 211
  SIP ALG 168
    activation 168
  traversal 212
  what it does 169
negotiation mode 215
Network Address Translation, see NAT
network map 26
non-proxy calls 232

O

OK response 237
other documentation 2
outside header 213

P

Pairwise Master Key (PMK) 342, 343
passphrase 100
passwords 23
PBC 114
peer-to-peer calls 232
Per-Hop Behavior, see PHB
PHB 160, 238
phone book
  speed dial 232
PIN, WPS 114
  example 115
ports 20
PPP over Ethernet, see PPPoE
PPPoE 82, 91
  Benefits 91
preamble 110
preamble mode 337
prefix delegation 84
pre-shared key 217
Printer Server 131
printer sharing
  and LAN 131
  configuration 50
  requirements 131
  TCP/IP port 50
product registration 372
profile 35
protocol 82
PSK 342
PSTN call setup signaling 237
pulse dialing 237
Push Button Configuration, see PBC
push button, WPS 114

Q

QoS 149, 150, 160, 238
Quality of Service, see QoS
Quick Start Guide 2, 23

R

RADIUS 338
  message types 339
  messages 339
  shared secret key 339
RADIUS server 111
Real time Transport Protocol, see RTP
registration
  product 372
related documentation 2
Request To Send, see RTS
reset 269
RESET button 22
restart 269
restoring configuration 268
RFC 1631 161
RFC 1889 236
RFC 3164 243
router advertisements 84
RTP 236
RTS (Request To Send) 336
  threshold 335, 336
RTS threshold 110

S

scan 98
scheduling
  wireless LAN 108
secure gateway address 202
security
  wireless LAN 110
security associations, see VPN
security, network 184
service access control 256
Service Set 98, 105
Session Initiation Protocol, see SIP
setup
  firewalls 178
silence suppression 222
SIP 233
  account 233
  call progression 236
  client 234
  identities 233
  INVITE request 237
  number 233
  proxy server 235
  redirect server 235
  register server 236
  servers 234
  service domain 234
  URI 233
  user agent 234
SIP ALG 168
  activation 168
speed dial 232
SSID 111
  activation 104
static route 145
static VLAN
status 75
status indicators 20
subnet 283
subnet mask 133, 284
subnetting 286
supplementary services 239
syslog
  protocol 243
  severity levels 243
system
  firmware 265
  passwords 23
  status 75
System Info 77
system name 77, 260

T

Tag Control Information See TCI
Tag Protocol Identifier See TPID
TCI
TCP/IP port 50
Temporal Key Integrity Protocol, see TKIP
The 82
three-way conference 241

thresholds
data fragment 110
RTS/CTS 110
TKIP 341
ToS 238
TPID 92
trademarks 369
trusted CAs, and certificates 195
tunnel mode 213
tutorial
VoIP 39
wireless 31
Type of Service, see ToS

U

unicast 92
Uniform Resource Identifier 233
Universal Plug and Play, see UPnP
upgrading firmware 265
UPnP 127
forum 122
security issues 122

V

VAD 222
version
firmware
version 77
VID
Virtual Local Area Network See VLAN
Virtual Local Area Network, see VLAN
Virtual Private Network, see VPN
VLAN 91, 239
group 239
ID 239
ID tags 239
Introduction 91
number of possible VIDs
priority frame
static
VLAN ID 92
VLAN Identifier See VID
VLAN tag 92
voice activity detection 222
voice coding 237
VoIP 233
features 18
peer-to-peer calls 232
tutorial 39
VoIP features 18
VoIP status 251
VPN 201
established in two phases 201
IPSec 201
security associations (SA) 201
see also IKE SA, IPSec SA

W

WAN
Wide Area Network, see WAN 81
warranty 371
note 371
Web Configurator 23
web configurator
passwords 23
WEP 100, 112
WEP Encryption 101
Wi-Fi Protected Access, see WPA
wireless
client configuration 33
profile 35
security 337
tutorial 31
wireless client WPA supplicants 342
wireless LAN 95
authentication 110, 111
BSS 113
example 113
channel 96
encryption 112
example 96
fragmentation threshold 110
limitations 112
MAC address filter 111
preamble 110

RADIUS server 111
RTS/CTS threshold 110
scheduling 108
security 110
SSID 111
activation 104
WEP 112
WPA 112
WPA-PSK 112
WPS 113, 116
example 117
limitations 118
PIN 114
push button 114
wireless network
example 95
wireless security 337
WLAN 95
auto-scan channel 98
interference 335
passphrase 100
scheduling 108
security parameters 344
see also wireless.
WEP 100
WLAN button 19
WPA 112, 341
key caching 342
pre-authentication 342
user authentication 342
vs WPA-PSK 342
wireless client supplicant 342
with RADIUS application example 343
WPA2 341
user authentication 342
vs WPA2-PSK 342
wireless client supplicant 342
with RADIUS application example 343
WPA2-Pre-Shared Key, see WPA2-PSK
WPA2-PSK 341, 342
application example 343
WPA-PSK 112, 341, 342
application example 343
WPS 113, 116
example 117
limitations 118
PIN 114
example 115
push button 114